TP-LINK®
The Reliable Choice

Auranet

User Guide

For TP-LINK Auranet Access Points

EAP115

REV1.0.0
1910011765

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

1) This device may not cause harmful interference.

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

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

CE1588

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

RF Exposure Information

This device meets the EU requirements (1999/5/EC Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

IC STATEMENT

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Canadian Compliance Statement

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

1） This device may not cause interference, and

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

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

1） l’appareil ne doit pas produire de brouillage;

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

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Declaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

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

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

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

EAC

Safety Information

- When product has power button, the power button is one of the way to shut off the product; When there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don’t disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.

Explanation of the symbols on the product label

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

NCC Notice & BSMI Notice

注意！

依據低功率電波輻射性電機管理辦法

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

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

減少電磁波影響，請妥適使用。

安全諮詢及注意事項

●請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。

●清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。

●注意防潮，請勿將水或其他液體潑灑到本產品上。

●插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。

●請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。

●請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

此為甲類資訊技術設備，于居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

CONTENTS

Chapter 1 About This Guide

This User Guide contains information for setup and management of EAP115. Please read this guide carefully before operation.

1.1 Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.

1.2 Conventions

When using this guide, please notice that features of the EAP may vary slightly depending on the model and software version you have, and on your location, language, and Internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

More Info:

- The latest software, management app and utility can be found at Download Center at *http://www.tp-link.com/support*.
- The Installation Guide (IG) can be found where you find this guide or inside the package of the EAP.
- Specifications can be found on the product page at *http://www.tp-link.com.*
- A Technical Support Forum is provided for you to discuss our products at *http://forum.tp-link.com.*
- Our Technical Support contact information can be found at the Contact Technical Support page at *http://www.tp-link.com/support.*

Chapter 2 Introduction

2.1 Overview of the EAP

EAP series products provide wireless coverage solutions for small-medium business. They can either work independently as standalone APs or implement centralized management, providing a flexible, richly-functional but easily-configured enterprise-grade wireless network for small and medium business.

"Celling lamp" appearance and easily mounting design with chassis make EAP easy to be installed on a wall or ceiling and blend in with most interior decorations. EAP115 can be powered via a PSE* device or the provided power adapter.

With two built-in omnidirectional antennas, EAP115 works within the 2.4GHz frequency band. It applies 802.11n standards and 2*2MIMO technology, allowing packet transmission at up to 300Mbps.

*PSE: Power Sourcing Equipment, a device (switch or hub for instance) that will provide power in a PoE setup.

2.2 Appearance Description

2.2.1 Top View

The top view of EAP115 is shown as the following figure.

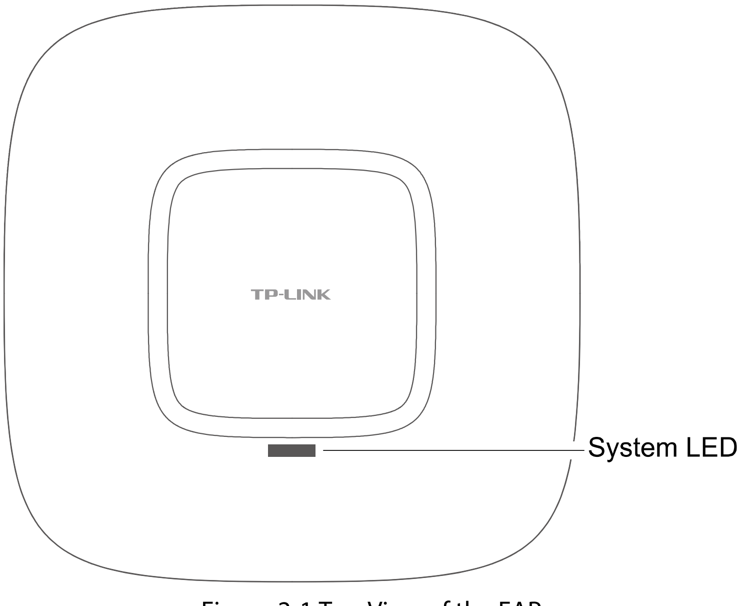


Figure 2-1 Top View of the EAP

- **LED**

  There is a System LED on the top of the EAP. The following table explains the indications of different LED colors.

LED Color	Indication
Flashing green	System initialization is complete.
Solid green	The device is working properly.
Flashing red	System errors. RAM, flash, Ethernet, WLAN or firmware may be malfunctioning.
Flashing yellow	Firmware update is in progress. Do not disconnect or power off the device.
Alternating red/green/yellow twice	The device is being reset.

2.2.2 Panel Layout

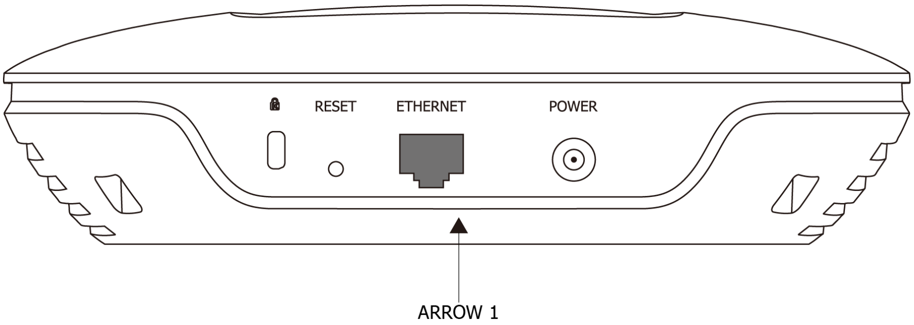


Figure 2-2 Panel Layout of the EAP

The interface panel components of the EAP, from left to right, are described in the following list:

- **Kensington Security Slot:** Secure the lock (not provided) into the security slot to prevent the device from being stolen.
- **RESET:** With the device powered on, press and hold the RESET button for about 8 seconds until the LED flashes Red/Green/Yellow alternatively twice, then release the button. The device will restore to factory default settings.
- **ETHERNET:** This port is used to connect to a router to transmit data or to a PSE device, such as a switch, for both data transmission and Power over Ethernet (PoE) through Ethernet cabling.
- **POWER:** The power port is used connect the device to an electrical wall outlet via power adapter. Please only use the provided power adapter.
- **ARROW 1:** This arrow is used to align with ARROW 2 on the mounting bracket to lock the EAP into place.

2.2.3 Mounting Bracket

The following figure describes the structure of the mounting bracket.

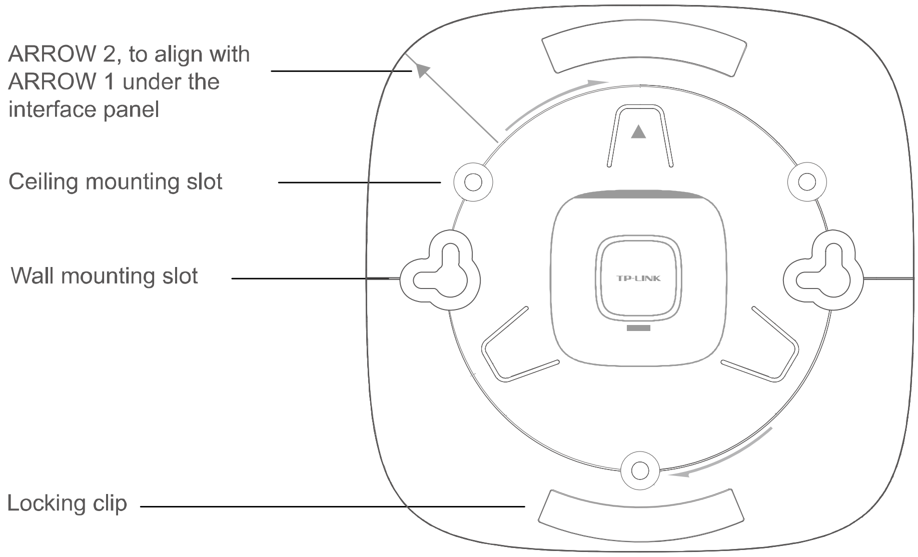


Figure 2-3 Structure of the Mounting Bracket

Chapter 3 Typical Topology

A typical topology for the EAP is described below.

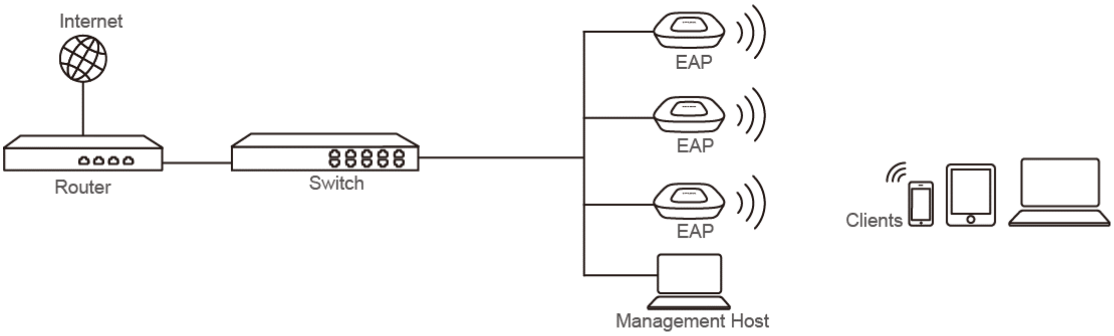


Figure 3-1 Typical Topology

To deploy an EAP in your local network, a DHCP server is required to assign IP addresses to the EAPs and clients. Typically, a router acts as the DHCP server.

Typically, you can choose a Power over Ethernet (PoE) switch to provide power for the EAP. You can also use the power adapter to provide power instead if the PoE switch is unavailable.

The EAP115 can be managed in three ways: **EAP Controller**, **Cluster** and **Standalone.**

EAP Controller: The EAP Controller software allows network administrators to monitor and manage hundreds of Auranet EAPs, at multiple sites, from any connected PC within the network. This dramatically enhances scalability and makes remote network management more convenient. For more information about the EAP Controller, please refer to the **EAP Controller User Guide** from our official website:

http://www.tp-link.com/en/support/download/

Cluster mode: In this mode, all the EAP115s with a same cluster name in a same LAN will form a cluster (the number of EAPs in a cluster is no more than 24), and a Master EAP will be elected among them to manage other EAPs which are called Member EAPs. On the management host, the access to any EAP's IP address will be redirected to the Master EAP's web management page, where you can manage each member EAP in the cluster.

Standalone mode: In this mode, the EAP works independently as a standalone access point. By entering the IP address of the standalone EAP, you can log in to its web interface and perform configurations. The EAP can only be managed by EAP Controller in Standalone mode.

Chapter 4 Getting Started with the EAP

The following content will guide you to quickly set up a wireless network connection with several EAPs, and login to the management page to configure the EAPs. The management host can be connected to the EAP wirelessly or with wires. Wireless Login is conveniently recommended.

EAP115 can be managed in three ways: **EAP Controller**, **Cluster** and **Standalone.** In this User Guide, we introduce Cluster Mode and Standalone Mode.

Option 1: Wireless Login

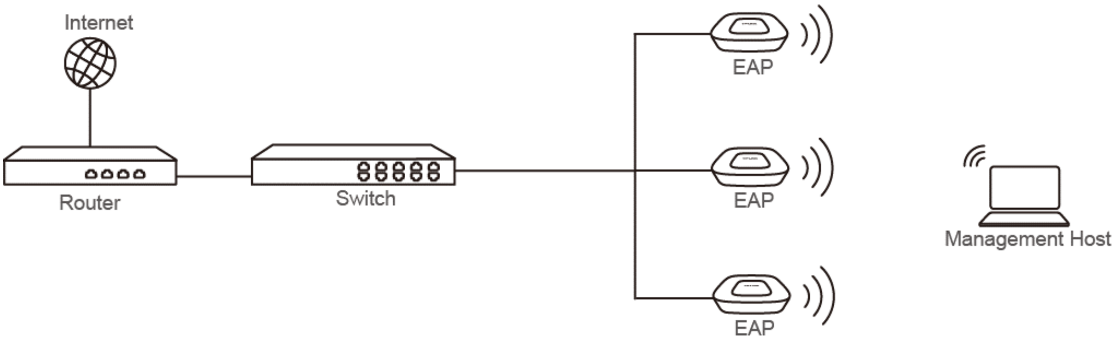


Figure 4-1 Sample Network Diagram for Wireless Login

Step 1: Power on

Power on the EAPs.

Step 2: Wireless Access

1. Make sure the management host is set to **obtain IP address automatically**.
2. Join the wireless network using the default SSID TP-LINK_2.4GHz_XXXXXX, where XXXXXX represents the last 6 characters of the EAP's MAC address. Password is not required.

Step 3: Choose the work mode

1. Open a web browser and type in http://tplinkeap.net to access the EAP's web management page. The default user name and password are **admin** (all lowercase).
2. Choose the work mode in the drop-down box the first time you login. With factory default settings, the EAP works in Standalone mode.
3. Configure the EAP parameters. Please refer to the corresponding chapter according to the work mode you chose.

Congratulations! Now you can enjoy the wireless network.

If you want to perform more configurations, please connect to the new SSID.

Option 2: Wired Login

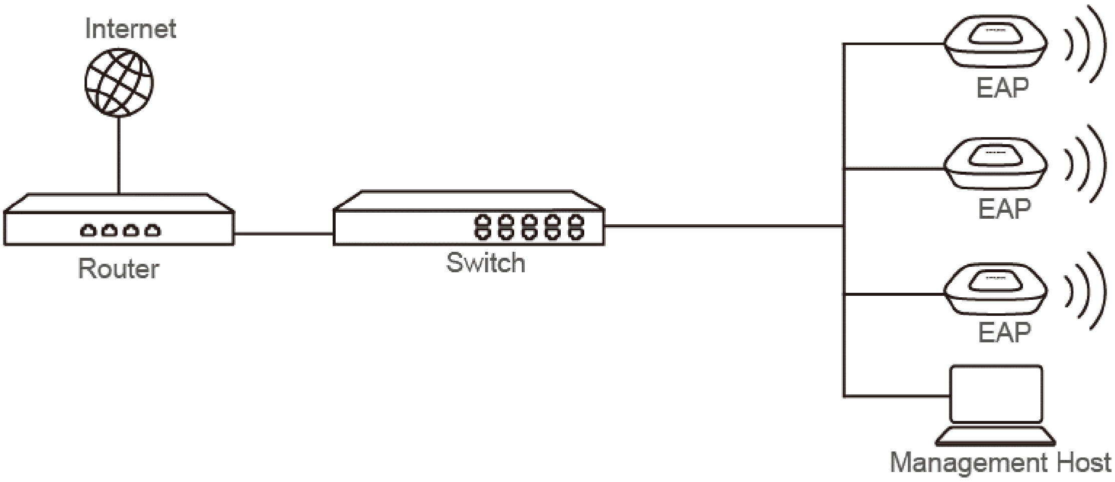


Figure 4-2 Sample Network Diagram for Wired Login

Step 1: Power on

Power on the EAPs.

Step 2: Wired Access

1. Make sure the management host is set to **obtain IP address automatically**.
2. Access your DHCP server and locate the IP address of the EAPs.

Step 3: Choose the work mode

1. Open a web browser, in the address field type in the IP address of the EAP to access the EAP's web management page. The default user name and password are **admin** (all lowercase).
2. Choose the work mode in the drop-down box the first time you login. With factory default settings, the EAP works in Standalone mode.
3. Configure the EAP parameters. Please refer to the corresponding chapter according to the work mode you chose.

Congratulations! Now you can enjoy the wireless network.

Chapter 5 Management Mode

The Cluster mode is recommended for the centralized management of EAPs in a medium wireless network (the number of EAPs is no more than 24) if you don't want to install the EAP Controller. In Cluster mode, all the EAPs in this network can work in AP operating mode to provide wireless access service.

The Standalone mode applies to a relatively small-sized wireless network. EAPs in the Standalone mode cannot be managed centrally.

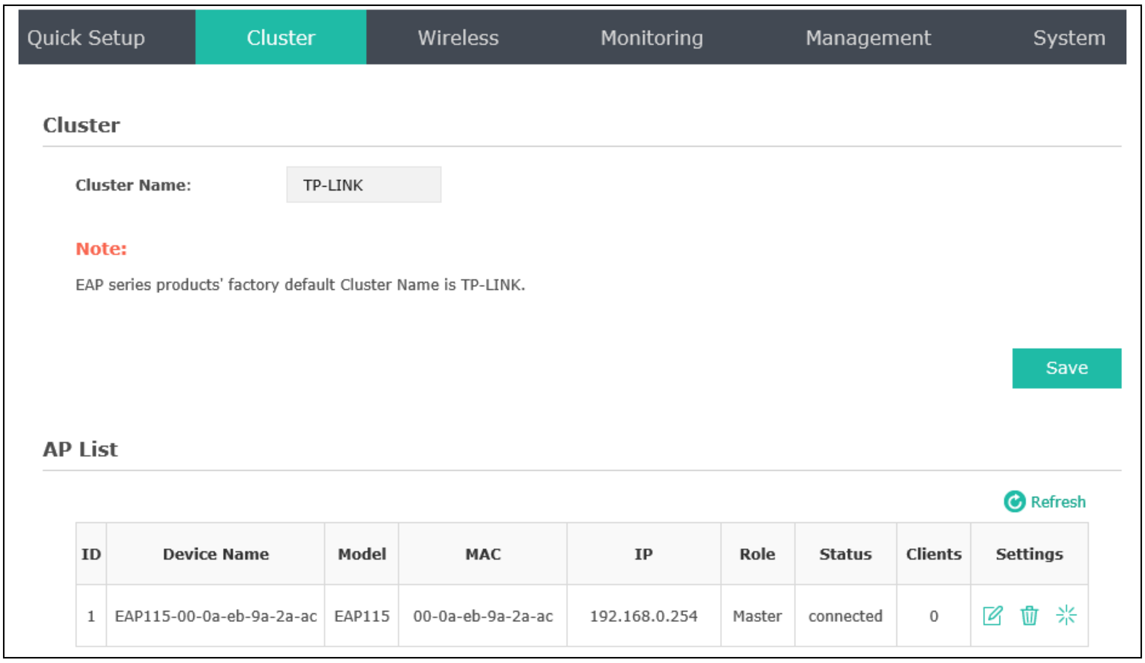
With factory default settings, the EAP works in Standalone mode. Switch the two management modes of the EAP based on the actual situations.

5.1 Mode Identification

How to judge the current management mode of the EAP? The web management pages of the EAP in the Cluster and Standalone mode are different. In Cluster mode, there is a Cluster tab, while in Standalone mode, there is a Network tab as shown below.

- ### Cluster

The web management page of the EAP in Cluster mode.



Cluster

Cluster Name: TP-LINK

Note:

EAP series products' factory default Cluster Name is TP-LINK.

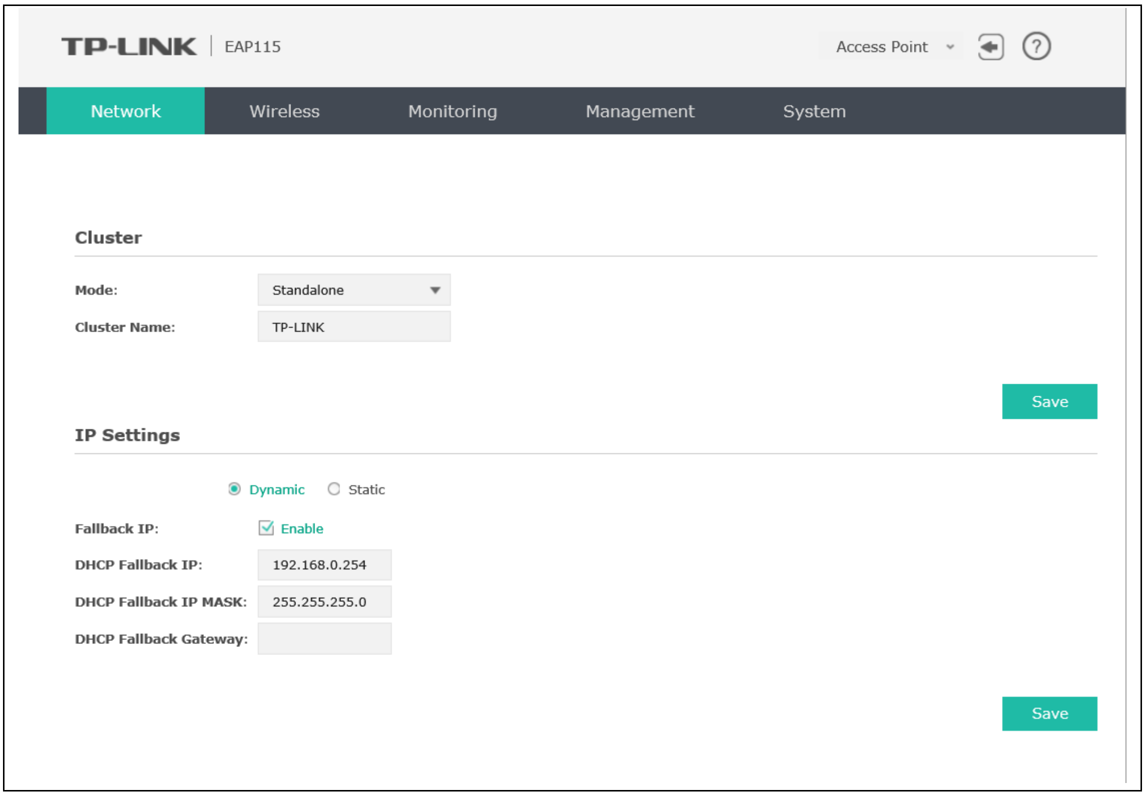
AP List

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Figure 5-1 Web Management Page in Cluster Mode

- **Standalone**

The web management page of the EAP in Standalone mode.



Cluster

Mode: Standalone

Cluster Name: TP-LINK

IP Settings

● Dynamic ○ Static

Fallback IP: ☑ Enable

DHCP Fallback IP: 192.168.0.254

DHCP Fallback IP MASK: 255.255.255.0

DHCP Fallback Gateway:

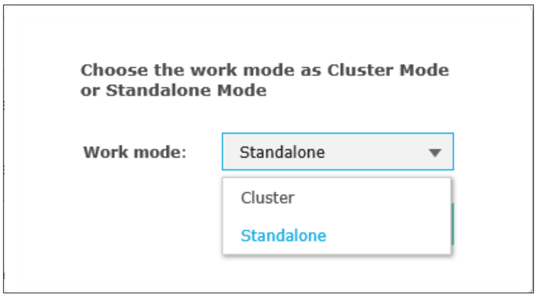
Figure 5-2 Web Management Page in Standalone Mode

5.2 Mode Switching

The management mode Cluster and Standalone can be switched with each other on every single EAP. The switching operation is shown below.

5.2.1 Choose the Work Mode the First Time You Login

Choose the work mode in the drop-down box the first time you log in. With factory default settings, the EAP works in Standalone mode. When you choose the work mode as Cluster, the EAP will reboot and switch to Cluster mode.



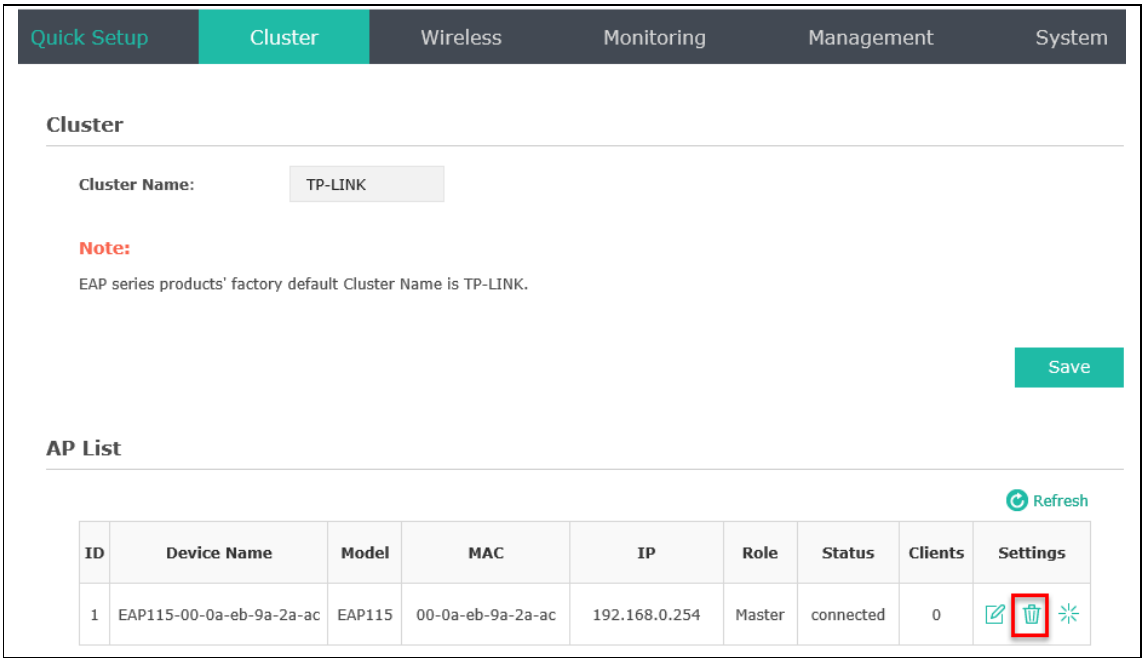
Choose the work mode as Cluster Mode or Standalone Mode

Work mode: Standalone

Figure 5-3 Choose the work mode

5.2.2 Switch from Cluster to Standalone

Log in to the web management page, click **Cluster** in the navigation tab when the EAP works in Cluster mode. AP List will be displayed as shown below.



Cluster

Cluster Name: TP-LINK

Note:
EAP series products' factory default Cluster Name is TP-LINK.

AP List

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Figure 5-4 Delete an EAP from a Cluster

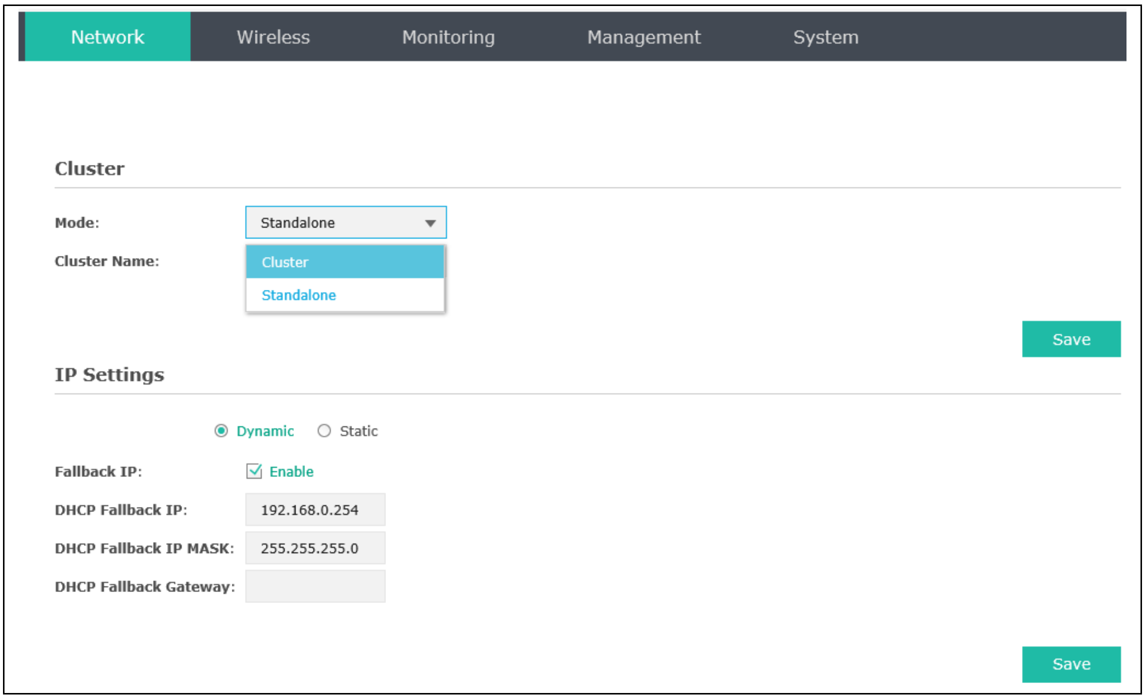
1. Select the specified EAP in the AP list and click the 🗑 icon in the Settings column.
2. If the deleted EAP is a Member (shown in the Role column) in the cluster, the mode will switch to Standalone. To know how to log in to the Member's web management page, refer to Chapter 4 Getting Started with the EAP. If the deleted EAP is a Master in the cluster, the management mode will switch to Standalone and the login window will pop up.

NOTE:

For detailed information of the Master EAP and Member EAP, please refer to 6.2 Cluster.

5.2.3 Switch from Standalone to Cluster

Log in to the web management page, click **Network** in the navigation tab when the EAP works in Standalone mode. The following content will be displayed.



Cluster

Mode: Standalone

Cluster Name:

IP Settings

● Dynamic ○ Static

Fallback IP: ☑ Enable

DHCP Fallback IP: 192.168.0.254

DHCP Fallback IP MASK: 255.255.255.0

DHCP Fallback Gateway:

Figure 5-5 Join a Cluster

1. Select the Mode as Cluster and enter a cluster name to join the cluster.

2. Click **Save** and the EAP will reboot and search the cluster with the same cluster name to join. If there is no device with the same cluster name in the network, the EAP will create a new cluster with this name and act as the Master.

Chapter 6 Cluster Mode

Cluster feature provides centralized management and monitoring of the EAPs, thus significantly simplifying the wireless network configuration and maintenance.

By default, the EAPs with a same cluster name and in a same subnet will form a cluster automatically. One EAP will be elected as the Master EAP, through which you can manage all the EAPs in this cluster centrally, while the other EAPs work as Members.

Master election determines the role of the cluster members. Master election is held each time the cluster is newly formed or the former Master works abnormally.

The Master is elected based on the following rules in the order listed:

1. **System Uptime**: The EAP with the longest system uptime becomes the Master. Uptime is the time that has elapsed since the last reboot.
2. **MAC Address**: The EAP with the highest MAC address becomes the Master.

In a cluster, the access to any EAP's IP address in the web browser will be redirected to the Master EAP's management web page. Each EAP's private parameters such as Name, Radio, IP Settings, Load Balance and SSID Override can be customized in the AP list in Cluster page, while the global configurations including Wireless, Monitoring, Management and System on the Master EAP will be automatically synchronized across the cluster to all Member EAPs.

NOTE:

You can remove the EAP from the cluster and switch it to Standalone mode if it is no longer planned to be managed by the cluster.

To form a cluster, make sure the following prerequisites or conditions are satisfied:

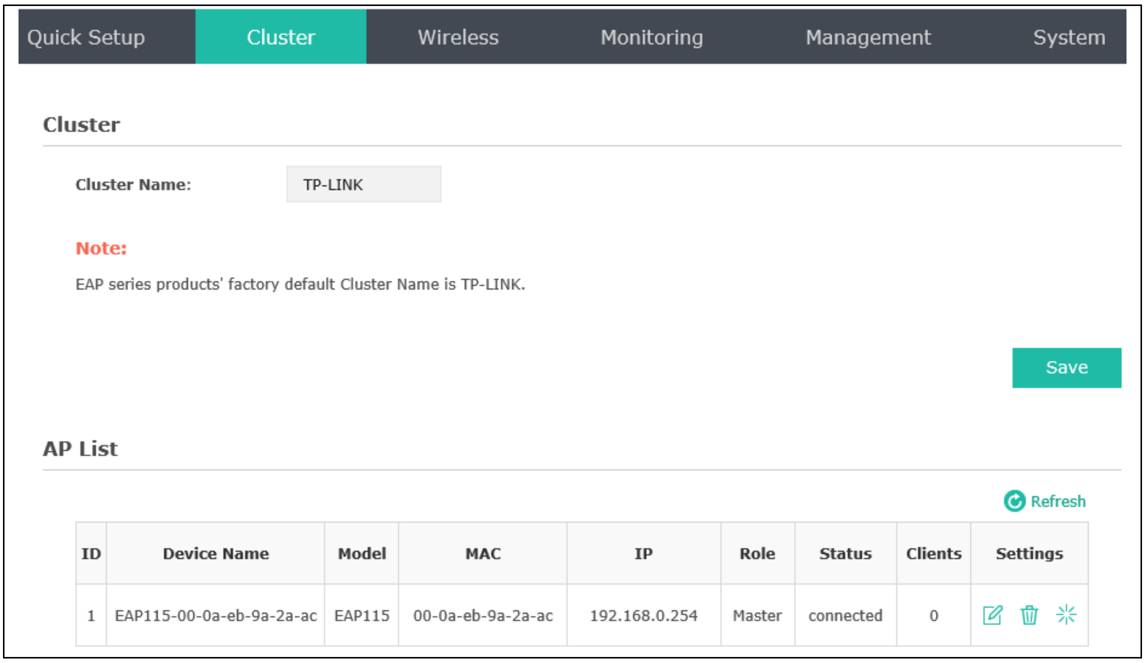
1. Be sure the EAPs forming a cluster are of the same model.
2. Be sure all EAP devices prepared for a cluster are in the same network segment.
3. Be sure the number of EAPs in a cluster is no more than 24.
4. Be sure all EAP devices prepared for a cluster have the same cluster name. It is recommended to specify a new cluster name to prevent malicious EAPs from joining and even becoming Master of the cluster.

6.1 Quick Setup

Follow the step-by-step instructions to complete the Quick Setup. Any configurations you make on the Master EAP will automatically synchronize to all the other EAPs.

6.2 Cluster

The Cluster page is shown below.



Cluster

Cluster Name: TP-LINK

Note:

EAP series products' factory default Cluster Name is TP-LINK.

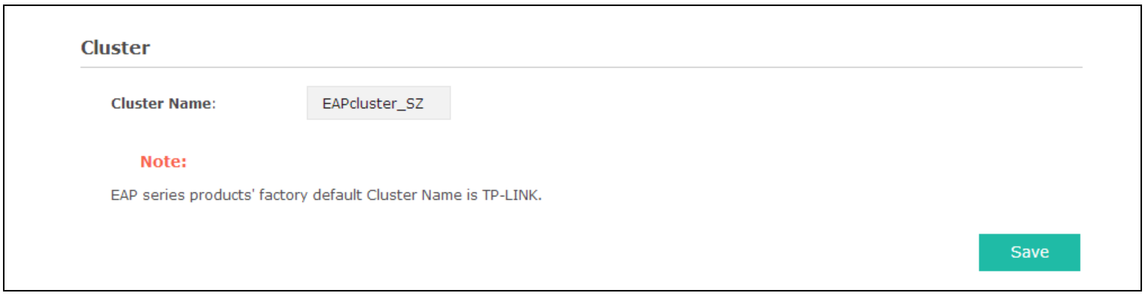
AP List

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Figure 6-1 Cluster Page

6.2.1 Cluster

Customize the cluster name in this zone. The cluster name will be synchronized automatically across the cluster to all Member EAPs. The EAPs have to have the same cluster name to form a cluster.



Cluster

Cluster Name: EAPcluster_SZ

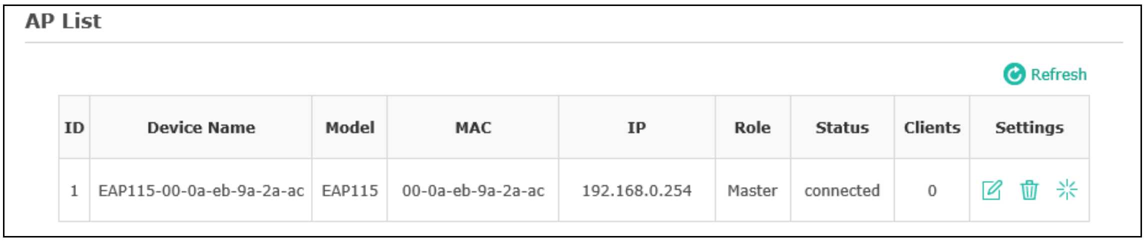
Note:

EAP series products' factory default Cluster Name is TP-LINK.

Figure 6-2 Modify the Cluster Name

6.2.2 AP List

AP List displays all the EAPs in this cluster. Click 📝 in the Settings column to configure the private parameters of the selected EAP. These private parameters take effect on each EAP separately, which helps to optimize the network performance. Configurable parameters include Device Name, Radio, IP Settings, Load Balance and SSID Override.



AP List

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	✎ 🗑 ✳

Figure 6-3 AP List

Device Name: Displays the name of the device. The default format of device name is "model-MAC address" (such as EAP115-00-0a-eb-9a-2a-ac).

Model: Displays the model of the device.

MAC: Displays the MAC address of the device.

IP: Displays the IP address of the EAP. By default, it is obtained from a DHCP server (typically a router).

Role: Displays the role of the EAP in a cluster, including Master and Member.

Status: Displays the status of an EAP in a cluster, including connected and joining.

- **Connected**: The EAP has joined a cluster.
- **Joining**: The EAP is trying to join a cluster.

Clients: Displays the number of wireless devices connected to the EAP.

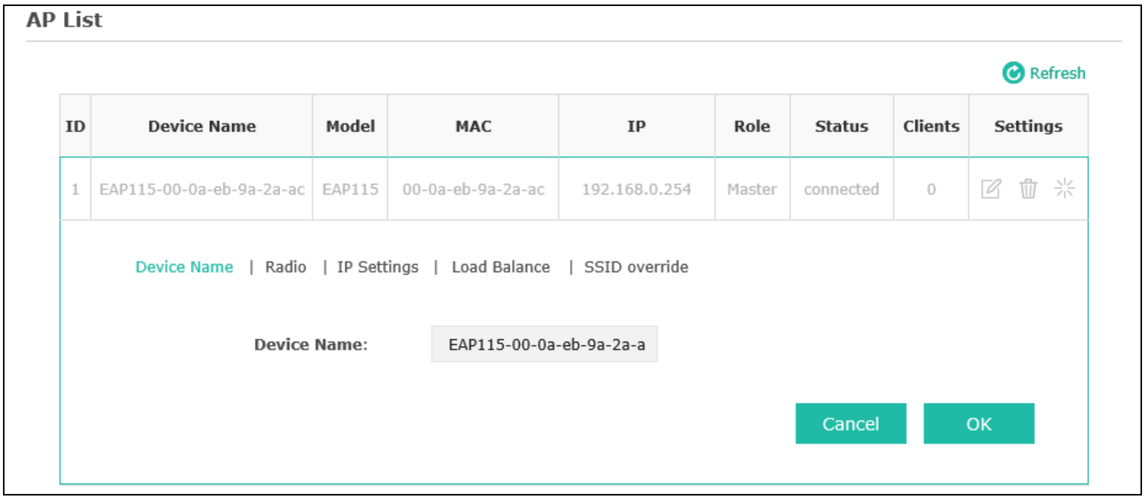
Settings: Operations here are only valid for a specific EAP.

✎: Click to configure the parameters of the EAP.

🗑: Click to remove the EAP from the cluster, thus the management mode of the removed EAP will switch to Standalone.

✳: Click to reboot the EAP.

Click ✎ to configure the wireless parameters of a specific EAP. The following content will be shown.



AP List

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	✎ 🗑 ✳

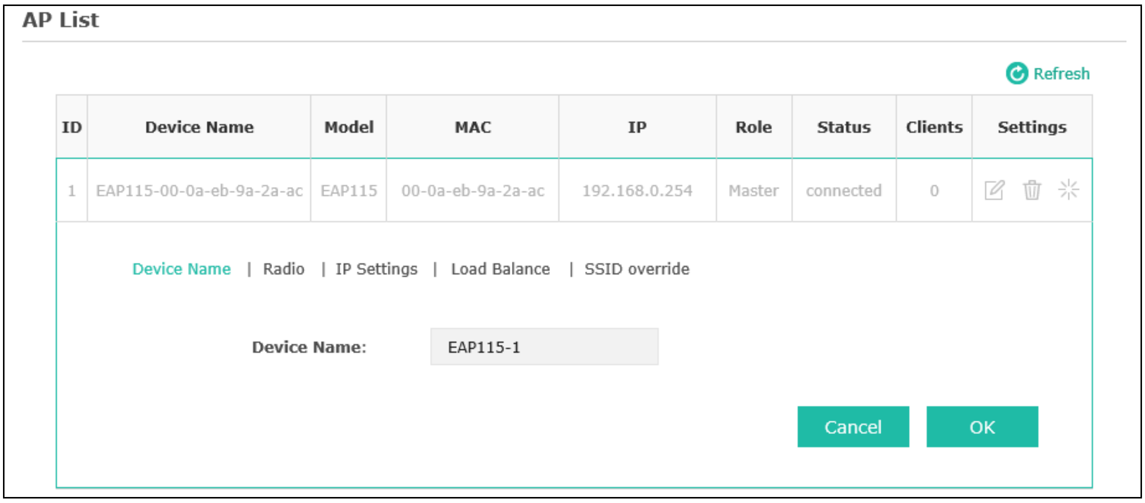
Device Name | Radio | IP Settings | Load Balance | SSID override

Device Name: EAP115-00-0a-eb-9a-2a-a

Figure 6-4 Configure the Wireless Parameters

- ## Device Name

You can rename the EAP like "EAP115_1" to distinguish it from others. The name can be 1 to 31 characters long. Then click **OK**.

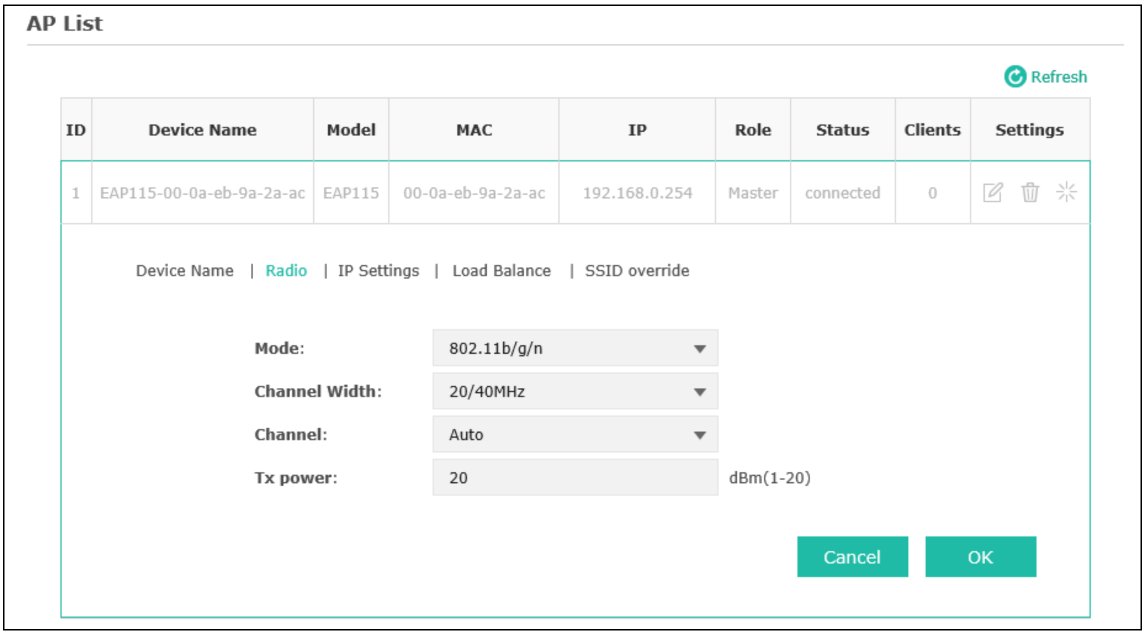

AP List
Refresh
Device Name | Radio | IP Settings | Load Balance | SSID override
Cancel
OK

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Device Name: EAP115-1

Figure 6-5 Rename the Device

- ## Radio


AP List
Refresh
Device Name | Radio | IP Settings | Load Balance | SSID override
Cancel
OK

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Mode: 802.11b/g/n

Channel Width: 20/40MHz

Channel: Auto

Tx power: 20 dBm(1-20)

Figure 6-6 Radio

Mode: Choose the protocol standard for the wireless network.

Wireless network created by EAP115 is able to operate in the 2.4GHz frequency, EAP115 supports 802.11b/g/n, 802.11b/g, and 802.11n standards. It is recommended to select 802.11b/g/n, in which way clients supporting 11b, 11g or 11n mode can access your wireless network.

Channel Width: Select the channel width of this device. Options include 20MHz, 40MHz and 20/40MHz (this device automatically selects 20MHz or 40MHz, and 20MHz will be used if 40MHz is not available). According to IEEE 802.11n standard, using a channel width of 40MHz can increase wireless throughput. However, users may choose lower bandwidth due to the following reasons:

1. To increase the available number of channels within the limited total bandwidth.
2. To avoid interference from overlapping channels occupied by other devices in the environment.
3. Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances.

Channel: Select the channel used by this device to improve wireless performance. 1/2412MHz means the Channel is 1 and the frequency is 2412MHz. The channel number varies in different regions. By default, channel is automatically selected.

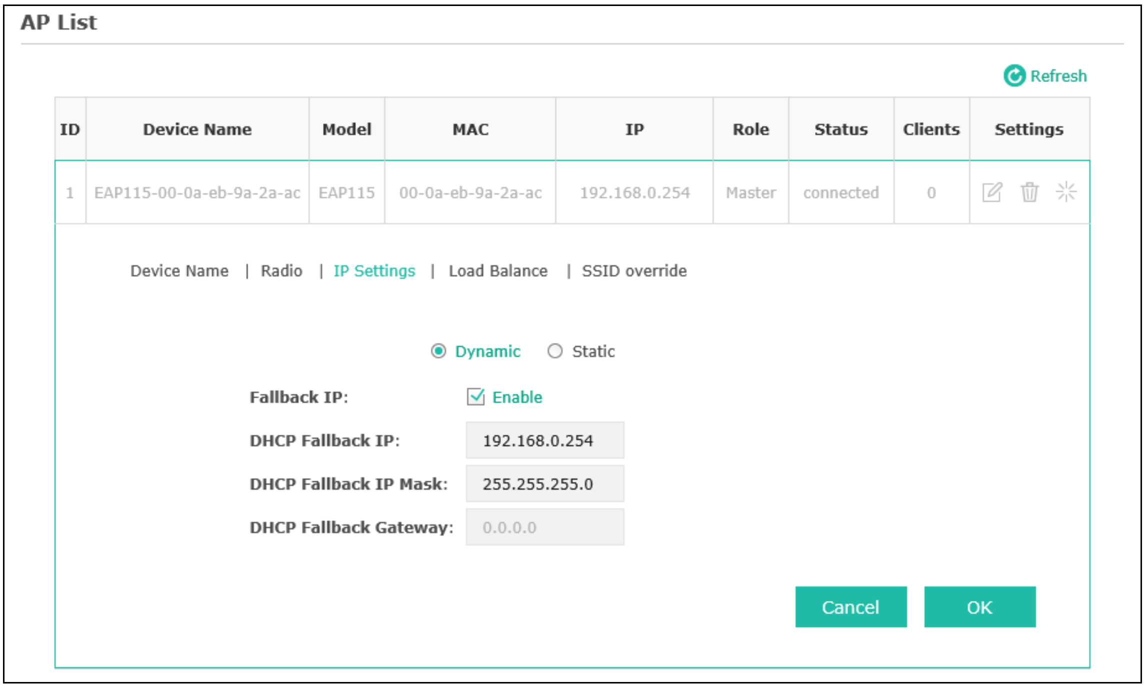
Tx Power: Enter the transmit power value. By default, the value is 20. The maximum transmit power may vary among different countries or regions.

If the maximum transmit power is set to be larger than local regulation allows, the maximum Tx power regulated will be applied in actual situation.

NOTE: In most cases, it is unnecessary to select maximum transmit power. Selecting larger transmit power than needed may cause interference to neighborhood. Also it consumes more power and will reduce longevity of the device. Select a certain transmit power is enough to achieve the best performance.

IP Settings

You can allocate the EAP a static IP address or set it to obtain an IP address automatically from a DHCP server. By default, the EAP is set to obtain IP address automatically, thus a DHCP server is required in the network.



ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Device Name | Radio | IP Settings | Load Balance | SSID override

● Dynamic ○ Static

Fallback IP: ☑ Enable

DHCP Fallback IP: 192.168.0.254

DHCP Fallback IP Mask: 255.255.255.0

DHCP Fallback Gateway: 0.0.0.0

Figure 6-7 IP Settings

Dynamic/Static: By default, the EAP device receives an IP address from a DHCP server (typically a router). Select Static to configure IP address manually.

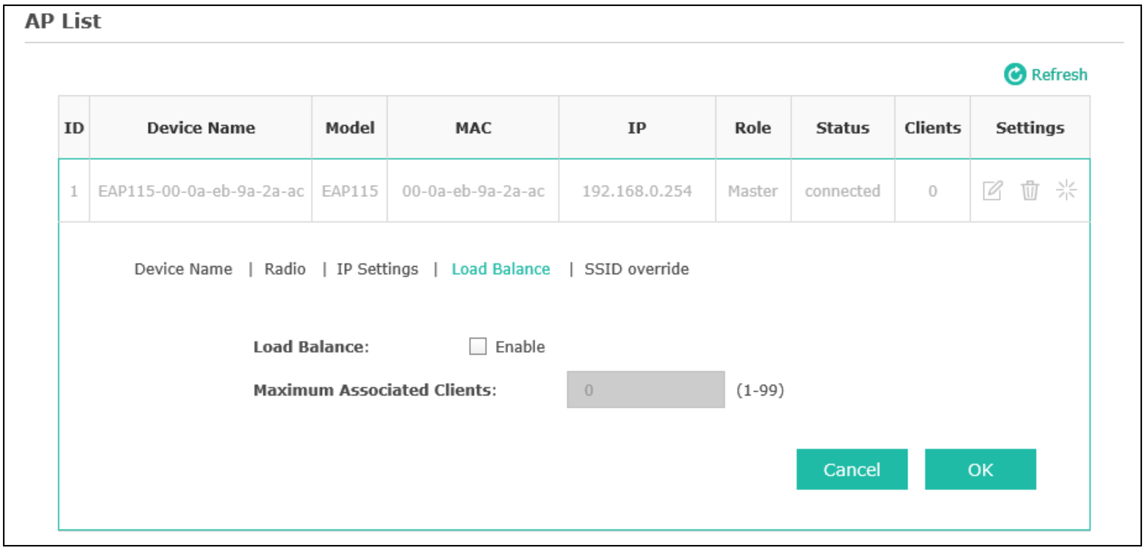
Fallback IP: If the EAP fails to get a dynamic IP address from a DHCP server within ten seconds, the fallback IP will work as the IP address of the device. After that, however, the device will keep trying to obtain an IP address from the DHCP until it succeeds.

DHCP Fallback IP/IP Mask: Enter the fallback IP/IP mask.

DHCP Fallback Gateway: Enter the fallback gateway.

- ## Load Balance

In a network with a great number of wireless clients, there may be a great disparity in the number of clients connected to each AP, which may waste the network resources and reduce the network performance. By restricting the maximum number of the wireless clients connected to an EAP, Load Balance helps to reduce the traffic loading and enhance the network performance.


AP List

Refresh

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Device Name | Radio | IP Settings | Load Balance | SSID override

Load Balance: □ Enable

Maximum Associated Clients: 0 (1-99)

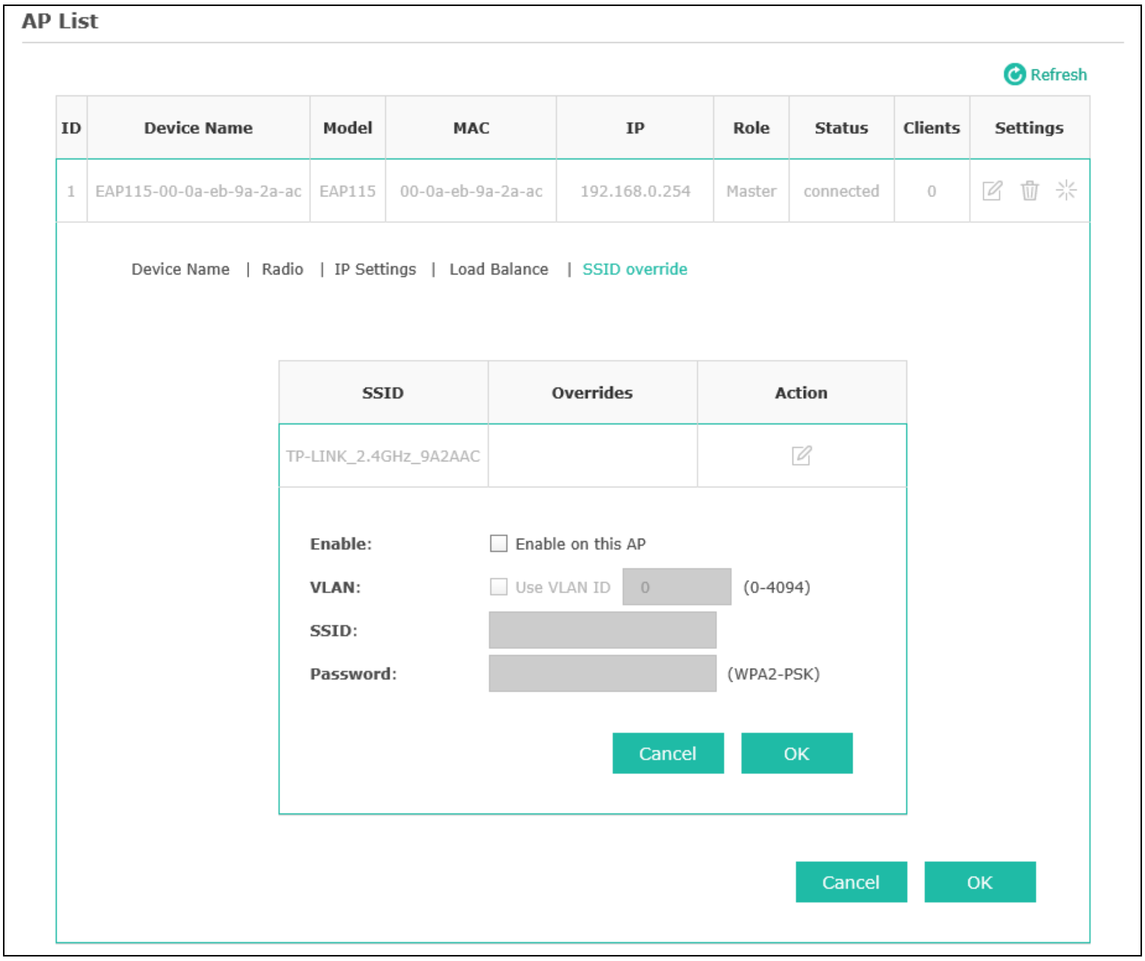
Figure 6-8 Load Balance

Load Balance:	Disable by default. Check the box to enable the function. Then you can set a number for maximum associated clients to control the wireless access.
Maximum Associated Clients:	Enter the number of clients to be allowed for connection to the EAP. The number ranges from 1 to 99.

- ## SSID Override

Customize the wireless network's SSID to distinguish it from the cluster's Service Set Identifier (SSID), which will help to locate this AP in the wireless network list. Meanwhile, wireless network can be divided into a specific VLAN based on the SSID. In a network with the same SSID, clients under the same VLAN can communicate with each other while clients of different VLANs are separated.

Click , the following content will be shown.



AP List

ID	Device Name	Model	MAC	IP	Role	Status	Clients	Settings
1	EAP115-00-0a-eb-9a-2a-ac	EAP115	00-0a-eb-9a-2a-ac	192.168.0.254	Master	connected	0	

Device Name | Radio | IP Settings | Load Balance | SSID override

SSID	Overrides	Action
TP-LINK_2.4GHz_9A2AAC		

Enable: □ Enable on this AP

VLAN: □ Use VLAN ID 0 (0-4094)

SSID:

Password: (WPA2-PSK)

Figure 6-9 SSID Override

Enable: Check the box to enable SSID Override.

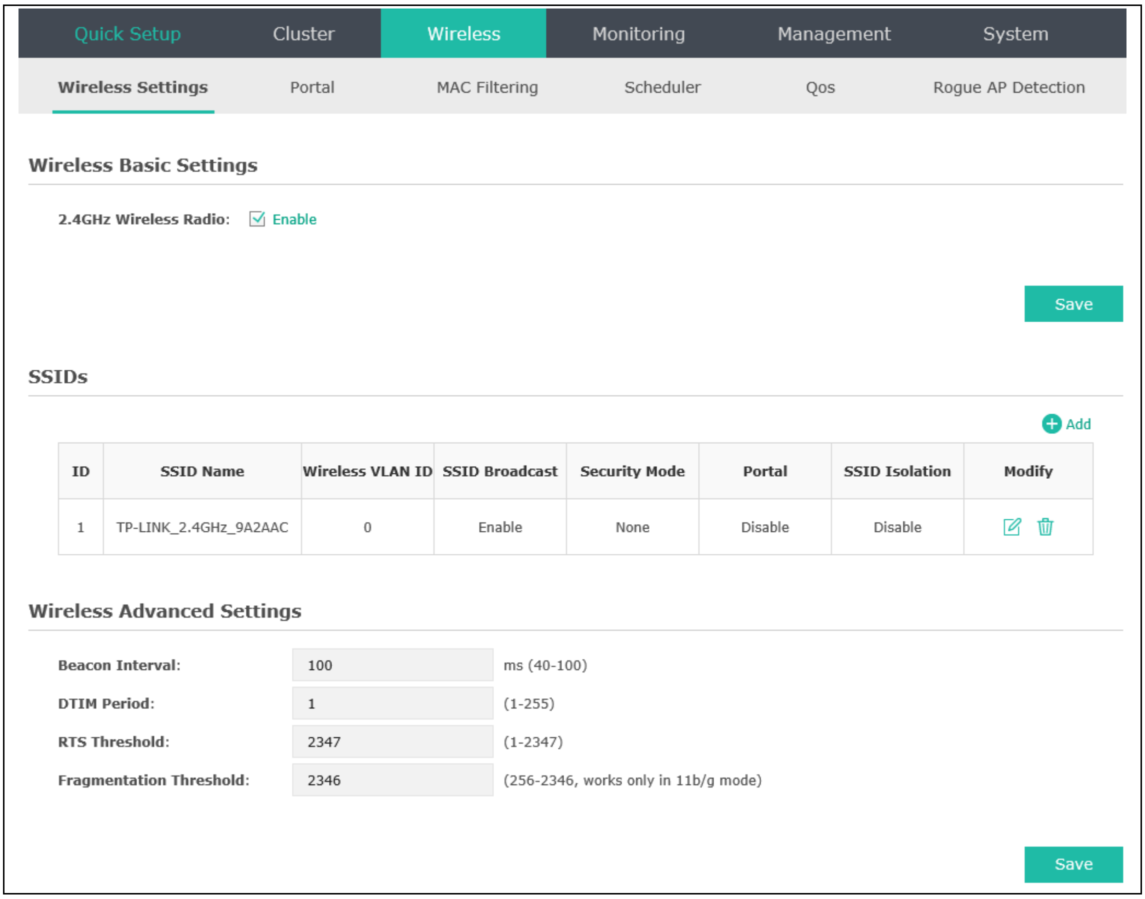
VLAN: Check the box to enable VLAN and set a VLAN ID (ranges from 0 to 4094) to the wireless network. VLAN 0 means VLAN function is disabled. Wireless networks with the same VLAN ID are grouped to a VLAN.

SSID: Enter an easily-identified SSID to override the SSID shared with other clustered EAPs.

Password: Set a WPA2-PSK password to access the wireless network. Only previous passwords with PSK encryption can be overridden.

6.3 Wireless

Wireless page, consisting of Wireless Settings, Portal, MAC Filtering, Scheduler, QoS and Rogue AP Detection, is shown below.



Wireless Basic Settings

2.4GHz Wireless Radio: ☑ Enable

Save

SSIDs

Add

ID	SSID Name	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-LINK_2.4GHz_9A2AAC	0	Enable	None	Disable	Disable	

Wireless Advanced Settings

Beacon Interval: 100 ms (40-100)

DTIM Period: 1 (1-255)

RTS Threshold: 2347 (1-2347)

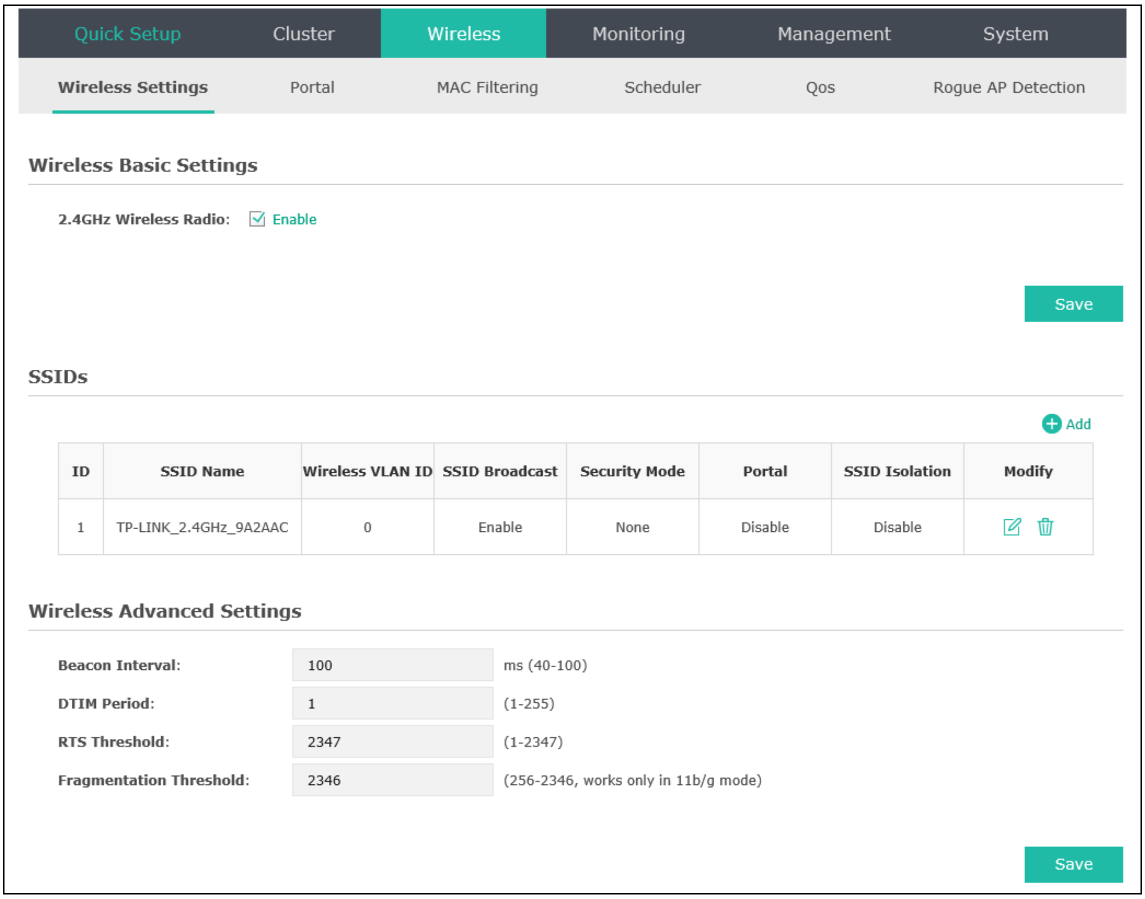
Fragmentation Threshold: 2346 (256-2346, works only in 11b/g mode)

Save

Figure 6-10 Wireless Page

6.3.1 Wireless Settings

Following is the page of Wireless Settings.



Wireless Basic Settings

2.4GHz Wireless Radio: ☑ Enable

Save

SSIDs

Add

ID	SSID Name	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-LINK_2.4GHz_9A2AAC	0	Enable	None	Disable	Disable	

Wireless Advanced Settings

Beacon Interval: 100 ms (40-100)

DTIM Period: 1 (1-255)

RTS Threshold: 2347 (1-2347)

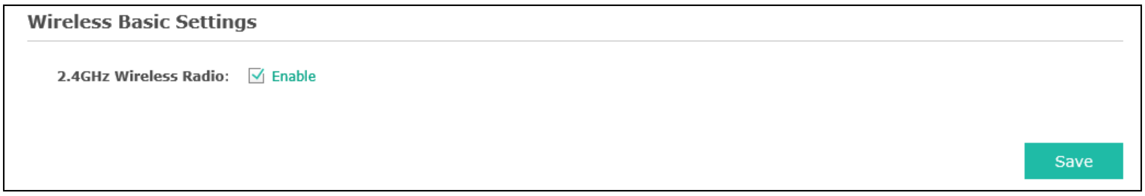
Fragmentation Threshold: 2346 (256-2346, works only in 11b/g mode)

Save

Figure 6-11 Wireless Settings Page

6.3.1.1 Wireless Basic Settings

In Cluter mode, parameters in Figure 6-15 including Wireless Mode, Channel Width, Channel and Tx Power are not available.


Wireless Basic Settings

2.4GHz Wireless Radio: ☑ Enable

Save

Figure 6-12 Wireless Basic Settings

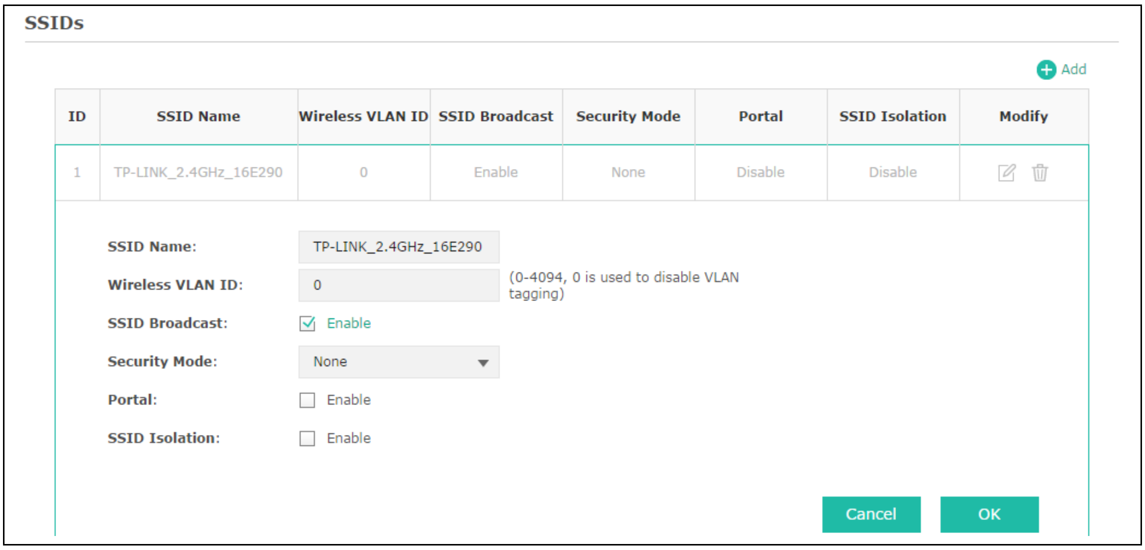
2.4GHz Wireless Radio: Check the box to enable 2.4GHz Wireless Radio.

6.3.1.2 SSIDs

SSIDs can work together with switches supporting 802.1Q VLAN. The EAP can build up to eight virtual wireless networks per radio for users to access. At the same time, it adds different VLAN tags to the clients which connect to the corresponding wireless network. It supports maximum 8 VLANs per radio. The clients in different VLAN cannot directly communicate with each other.

Clients connected to the device via cable do not belong to any VLAN. Thus wired client can communicate with all the wireless clients despite the VLAN settings.

Click ✎ in the Modify column, the following content will be shown.



SSIDs

+ Add

ID	SSID Name	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-LINK_2.4GHz_16E290	0	Enable	None	Disable	Disable	✎ 🗑

SSID Name: TP-LINK_2.4GHz_16E290

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

SSID Broadcast: ☑ Enable

Security Mode: None

Portal: □ Enable

SSID Isolation: □ Enable

Cancel OK

Figure 6-13 SSIDs

+ Add	Click to add up to 8 wireless networks per radio.
SSID Name:	Enter up to 32 characters as the SSID name.
Wireless VLAN ID:	Set a VLAN ID (ranges from 0 to 4094) for the wireless network. VLAN 0 means VLAN function is disabled. Wireless networks with the same VLAN ID are grouped to a VLAN.
SSID Broadcast:	Enable this function, AP will broadcast its SSID to hosts in the surrounding environment, as thus hosts can find the wireless network identified by this SSID. If SSID Broadcast is not enabled, hosts must enter the AP's SSID manually to connect to this AP.
Security Mode:	Select the security mode of the wireless network. For the safety of wireless network, you are suggested to encrypt your wireless network. This device provides three security modes: **WPA-Enterprise**, **WPA-PSK** (WPA Pre-Shared Key) and **WEP** (Wired Equivalent Privacy). WPA-PSK is recommended. Settings vary in different security modes as the details are in the following introduction. Select **None** and the hosts can access the wireless network without password.
Portal:	Portal provides authentication service for the clients who want to access the wireless local area network. For more information, refer to 6.4.2 Portal. After Portal is enabled, the configurations in 6.4.2 Portal will be applied.
SSID Isolation:	After enabling SSID Isolation, the devices connected in the same SSID cannot communicate with each other.

Modify: Click ✎ to open the page to edit the parameters of SSID.

Click 🗑 to delete the SSID.

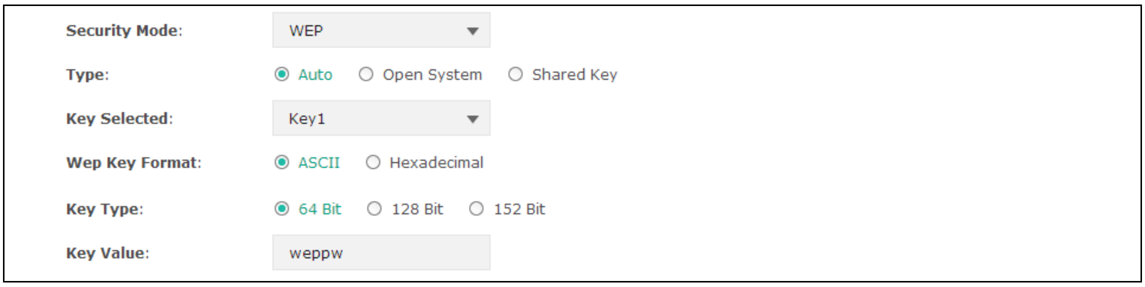
Following is the detailed introduction of security mode: **WEP**, **WPA-Enterprise** and **WPA-PSK**.

WEP

WEP (Wired Equivalent Privacy), based on the IEEE 802.11 standard, is less safe than WPA-Enterprise or WPA-PSK.

NOTE:

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



Security Mode: WEP

Type: ● Auto ○ Open System ○ Shared Key

Key Selected: Key1

Wep Key Format: ● ASCII ○ Hexadecimal

Key Type: ● 64 Bit ○ 128 Bit ○ 152 Bit

Key Value: weppw

Figure 6-14 Security Mode_WEP

Type: Select the authentication type for WEP.

- **Auto**: The default setting is Auto, which can select Open System or Shared Key automatically based on the wireless station's capability and request.
- **Open System**: After you select Open System, host in the wireless network can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission.
- **Shared Key**: After you select Shared Key, host in the wireless network has to input password to pass the authentication, or it cannot associate with the wireless network or transmit data.

Key Selected: You can configure four keys in advance and select one as the present valid key.

Web Key Format: Select the web key format ASCII or Hexadecimal.

- **ASCII**: ASCII format stands for any combination of keyboard characters in the specified length.
- **Hexadecimal**: Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

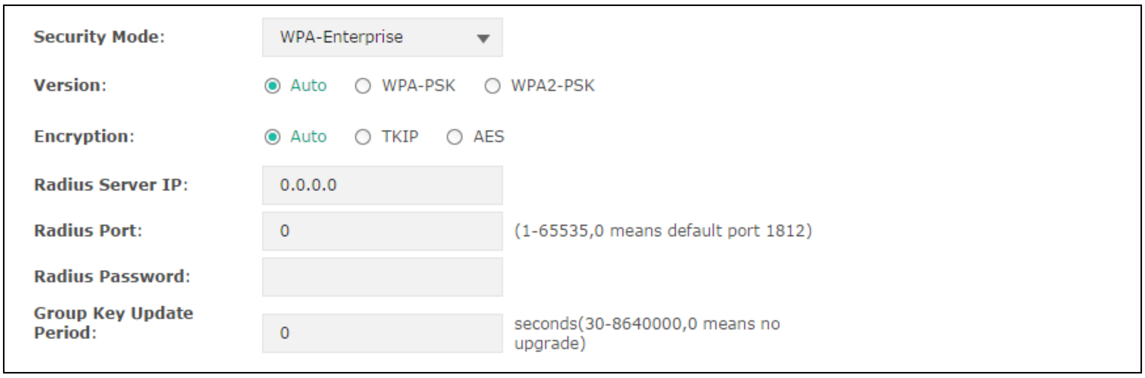
Key Type: Select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption.

- **64-bit**: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F without null key) or 5 ASCII characters.

	• **128-bit**: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F without null key) or 13 ASCII characters. • **152-bit**: You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F without null key) or 16 ASCII characters.
Key Value:	Enter the key value.

• WPA-Enterprise

Based on RADIUS server, WPA-Enterprise can generate different passwords for different users and it is much safer than WPA-PSK. However, it costs much to maintain and is more suitable for enterprise users. At present, WPA-Enterprise has two versions: WPA-PSK and WPA2-PSK.



Security Mode:	WPA-Enterprise ▼
Version:	● Auto ○ WPA-PSK ○ WPA2-PSK
Encryption:	● Auto ○ TKIP ○ AES
Radius Server IP:	0.0.0.0
Radius Port:	0 (1-65535,0 means default port 1812)
Radius Password:	
Group Key Update Period:	0 seconds(30-8640000,0 means no upgrade)

Figure 6-15 Security Mode_WPA-Enterprise

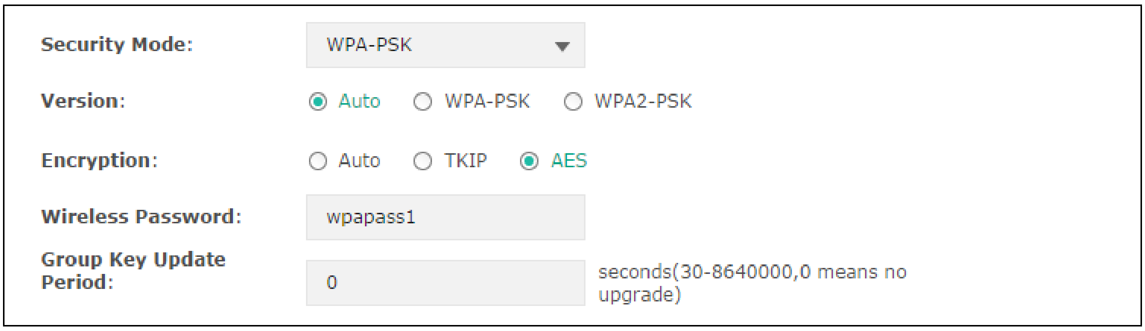
Version:	Select one of the following versions: • **Auto**: Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request. • **WPA-PSK**: Pre-shared key of WPA. • **WPA2-PSK**: Pre-shared key of WPA2.
Encryption:	Select the encryption type, including **Auto**, **TKIP**, and **AES**. The default setting is Auto, which can select TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) automatically based on the wireless station's capability and request. AES is more secure than TKIP and TKIP is not supported in 802.11n mode. It is recommended to select AES as the encryption type.
RADIUS Server IP/Port:	Enter the IP address/port of the RADIUS server.
RADIUS Password:	Enter the password to access the RADIUS server.
Group Key Update period:	Specify the group key update period in seconds. The value can be either 0 or at least 30. 0 means no update.

NOTE:

Encryption type TKIP is not supported in 802.11n mode. If TKIP is applied in 802.11n mode, the clients may not be able to access the wireless network of the EAP. If TKIP is applied in 11b/g/n mode (in the 2.4GHz frequency band), the device may work at a low transmission rate.

- ## WPA-PSK

Based on pre-shared key, security mode WPA-PSK is characterized by high safety and simple configuration, which suits for common households and small business. WPA-PSK has two versions: WPA-PSK and WPA2-PSK.

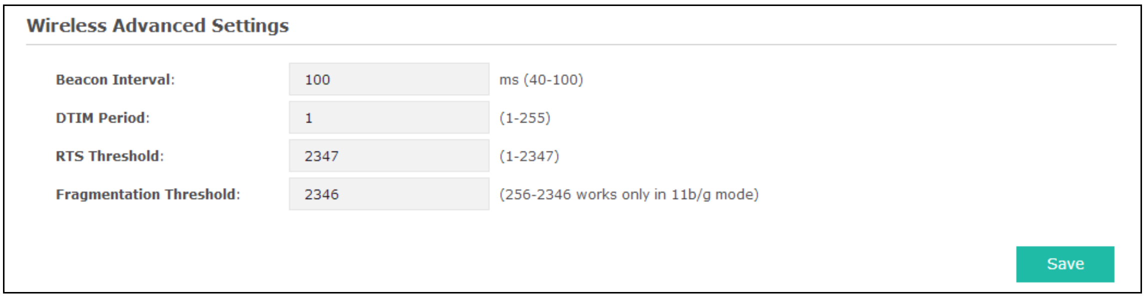


Security Mode:	WPA-PSK ▼
Version:	● Auto ○ WPA-PSK ○ WPA2-PSK
Encryption:	○ Auto ○ TKIP ● AES
Wireless Password:	wpapass1
Group Key Update Period:	0 seconds(30-8640000,0 means no upgrade)

Figure 6-16 Security Mode_WPA-PSK

Version:	• **Auto**: Select WPA or WPA2 automatically based on the wireless station's capability and request. • **WPA**: Pre-shared key of WPA. • **WPA2**: Pre-shared key of WPA2.
Encryption:	Select the encryption type, including **Auto**, **TKIP**, and **AES**. The default setting is Auto, which can select TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) automatically based on the wireless station's capability and request. AES is more secure than TKIP and TKIP is not supported in 802.11n mode. It is recommended to select AES as the encryption type.
Wireless Password:	Configure the WPA-PSK/WPA2-PSK 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 the group key update period in seconds. The value can be either 0 or at least 30. 0 means no update.

6.3.1.3 Wireless Advanced Settings



Wireless Advanced Settings

Beacon Interval:	100	ms (40-100)
DTIM Period:	1	(1-255)
RTS Threshold:	2347	(1-2347)
Fragmentation Threshold:	2346	(256-2346 works only in 11b/g mode)

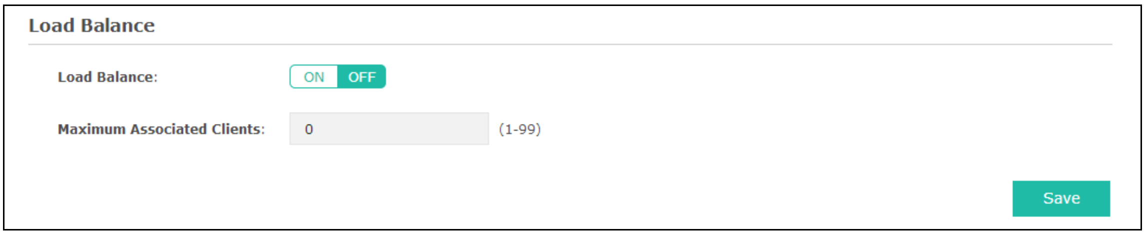
Figure 6-17 Wireless Advanced Settings

Beacon Interval:	Beacons are transmitted periodically by the 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 from 40 to 100. The default value is 100 milliseconds.
DTIM Period:	This value indicates the number of beacon intervals between successive Delivery Traffic Indication Messages (DTIMs) and this number is included in each Beacon frame. A DTIM is contained in Beacon frames to indicate whether the access point has buffered broadcast and/or multicast data for the client devices. Following a Beacon frame containing a DTIM, the access point will release the buffered broadcast and/or multicast data, if any exists. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating the DTIM Period is the same as Beacon Interval. An excessive DTIM period may reduce the performance of multicast applications. It is recommended to keep it by default.
RTS Threshold:	When the RTS threshold is activated, all the stations and APs follow the Request to Send (RTS) protocol. When the station is to send packets, it will send a RTS to AP to inform the AP that it will send data. After receiving the RTS, the AP notices other stations in the same wireless network to delay their transmitting of data. At the same time, the AP inform the requesting station to send data. The value range is from 1 to 2347 bytes. The default value is 2347, which means that RTS is disabled.
Fragmentation Threshold:	Specify the fragmentation threshold for packets. If the size of the packet is larger than the fragmentation threshold, the packet will be fragmented into several packets. Too low fragmentation threshold may result in poor wireless performance caused by the excessive packets. The recommended and default value is 2346 bytes.

6.3.1.4 Load Balance

Figure 6-21 is only displayed in Standalone mode. Load Balance in Cluster mode is explained in 6.2.2 AP List.

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


Load Balance

Load Balance: ON OFF

Maximum Associated Clients: 0 (1-99)

Figure 6-18 Load Balance

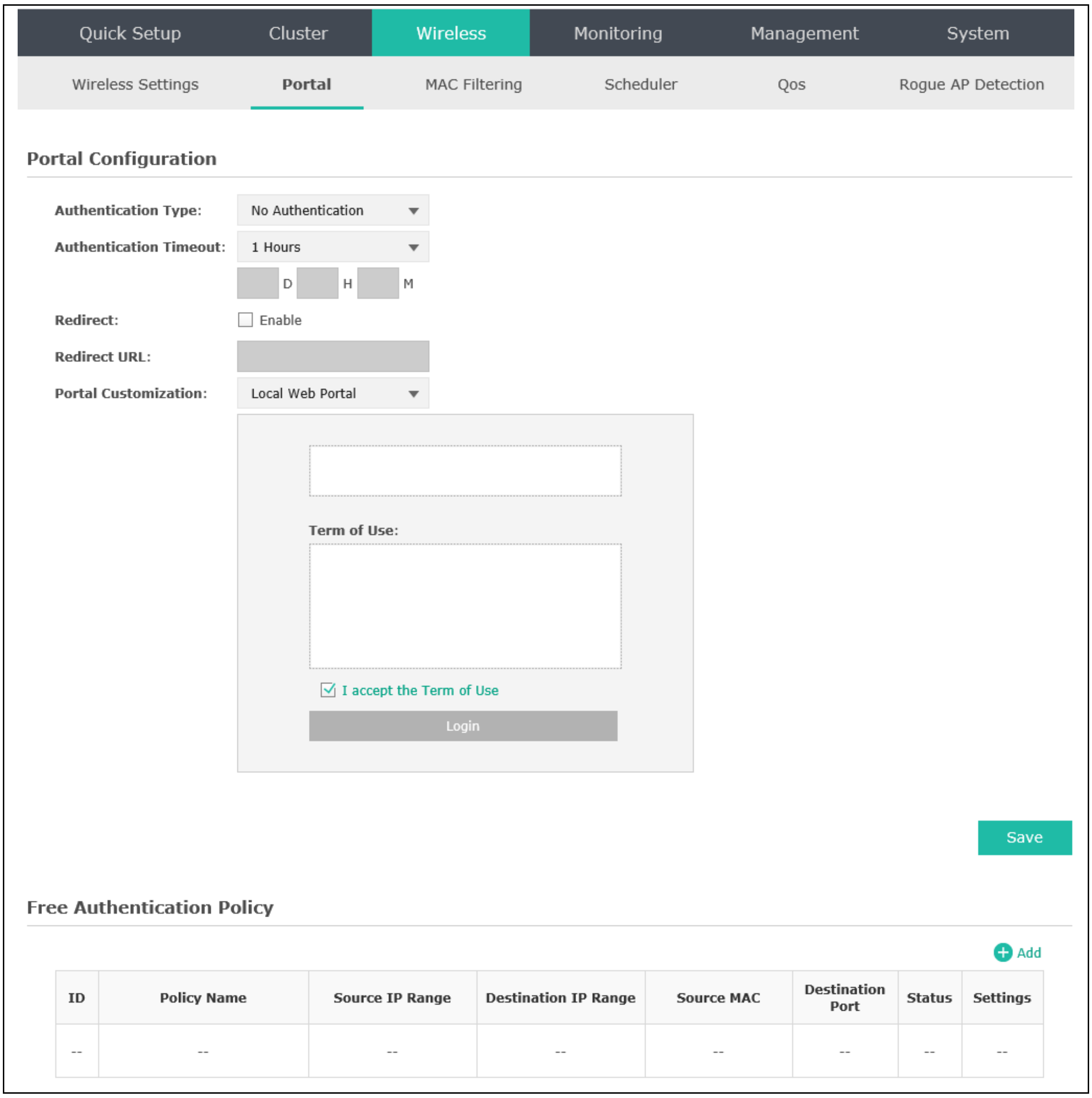
Load Balance:	Disable by default. Click **ON** to enable the function. After enabling it, you can set a number for maximum associated clients to control the wireless access.
Maximum Associated Clients:	Enter the number of clients to be allowed for connection to the EAP. The number ranges from 1 to 99.

6.3.2 Portal

Portal enhances the network security by providing authentication service to the clients who want to access the wireless local network. Portal is also called web authentication. The users have to log in a web page to establish verification.

Network resources can be classified into different types for different users. Part of them can be accessed for free by the clients; while some specific resources can only be accessed by authorized users. What's more, you can customize the authentication login page and specify a URL which the newly authenticated client will be redirected to. Please refer to Portal Configuration or Free Authentication Policy according to your need.

Following is the page of Portal.



Portal Configuration

Authentication Type: No Authentication

Authentication Timeout: 1 Hours

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal

Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Figure 6-19 Portal Page

NOTE:

To apply Portal in a wireless network, please go to **Wireless→Wireless Settings→SSIDs** to enable Portal of a selected SSID.

6.3.2.1 Portal Configuration

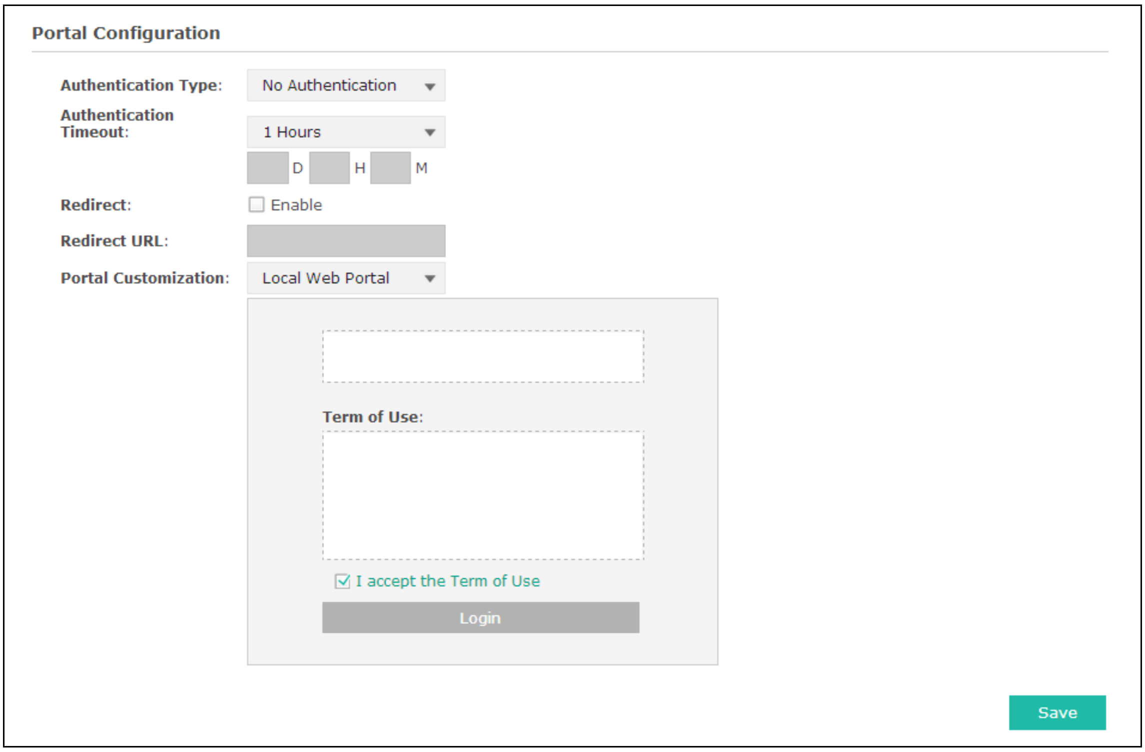
Three authentication types are available: No Authentication, Local Password and External RADIUS Server.

1. No Authentication： Users are required to finish only two steps: agree with the user protocol and click the **Login** button.
2. Local Password： Users are required to enter the preset user name and password, which are saved in the EAP.

3. External RADIUS Server：Users are required to enter the preset user name and password, which are saved in the database of the RADIUS server. The RADIUS server acts as the authentication server, which allows you to set different user name and password for different users.

Refer to the following content to configure Portal based on actual network situations.

- ## No Authentication



Portal Configuration

Authentication Type: No Authentication ▾

Authentication Timeout: 1 Hours ▾

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal ▾

Term of Use:

☑ I accept the Term of Use

Login

Save

Figure 6-20 Portal Configuration_No Authentication

Authentication Type: Select **No Authentication**.

Authentication Timeout: After successful verification, an authentication session is established. Authentication Timeout decides the active time of the session. Within the active time, the device keeps the authentication session open with the associated client. To reopen the session, the client needs to log in the web authentication page and enter the user name and password again once authentication timeout is reached.

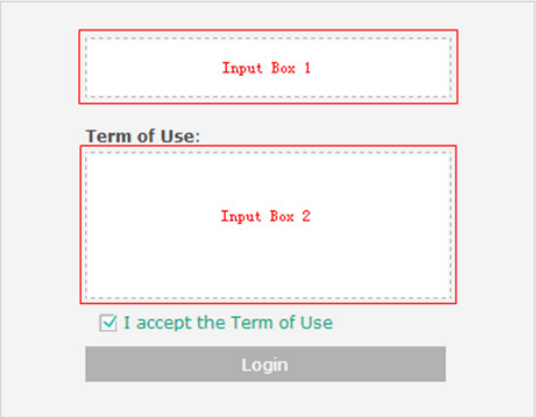
By default, authentication timeout is one hour. Select **Custom** from the drop-down list to customize the parameter.

Redirect: Disable by default. Redirect specifies that the portal should redirect the newly authenticated clients to the configured URL.

Redirect URL: Enter the URL that a newly authenticated client will be directed to.

Portal Customization: Select Local Web Portal, the authentication login page will be provided by the built-in portal server.

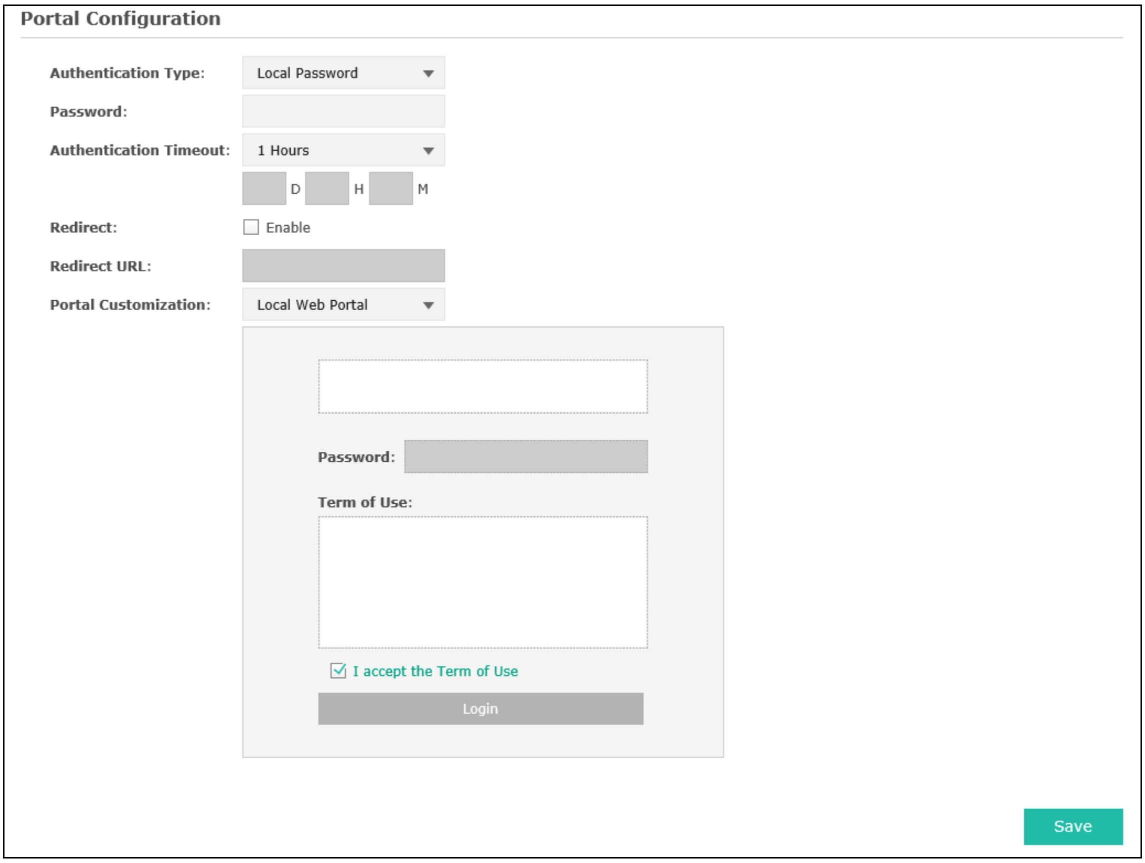
The page configured below will be presented to users as the login page. Words can be filled in Input Box 1 and Input Box 2.



Enter up to 31 characters as the title of the authentication login page in Input Box 1, like "Guest Portal of TP-LINK".

Enter the terms presented to users in Input Box 2. The terms can be 1 to 1023 characters long.

- ## Local Password



Portal Configuration

Authentication Type:	Local Password
Password:	
Authentication Timeout:	1 Hours
	D H M
Redirect:	□ Enable
Redirect URL:	
Portal Customization:	Local Web Portal

Figure 6-21 Portal Configuration_Local Password

Authentication Type: Select **Local Password**.

Password: Enter the password for local authentication.

Authentication Timeout: After successful verification, an authentication session is established. Authentication Timeout decides the active time of the session. Within active time, the device keeps the authentication session open with the associated client. To reopen the session, the client needs to log in the web authentication page and enter the user name and password again once authentication timeout is reached.

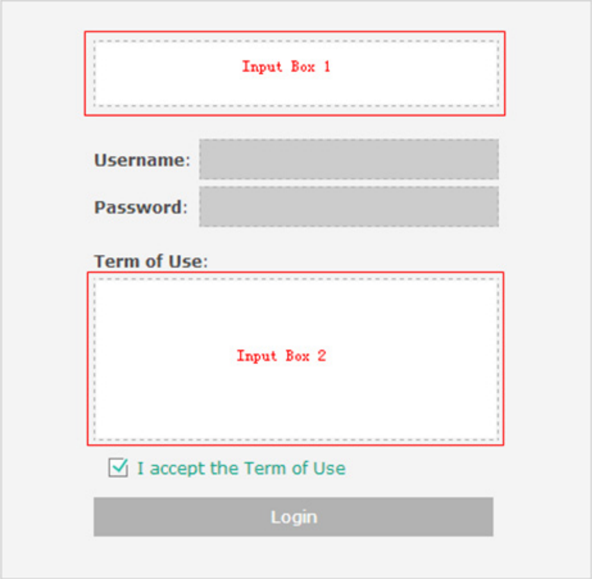
By default, authentication timeout is one hour. Select **Custom** from the drop-down list to customize the parameter.

Redirect: Disable by default. Redirect specifies that the portal should redirect the newly authenticated clients to the configured URL.

Redirect URL: Enter the URL that a newly authenticated client will be directed to.

Portal Customization: Select Local Web Portal, the authentication login page will be provided by the built-in portal server.

The page below will be presented to users. Words can be filled in Input Box 1 and Input Box 2.



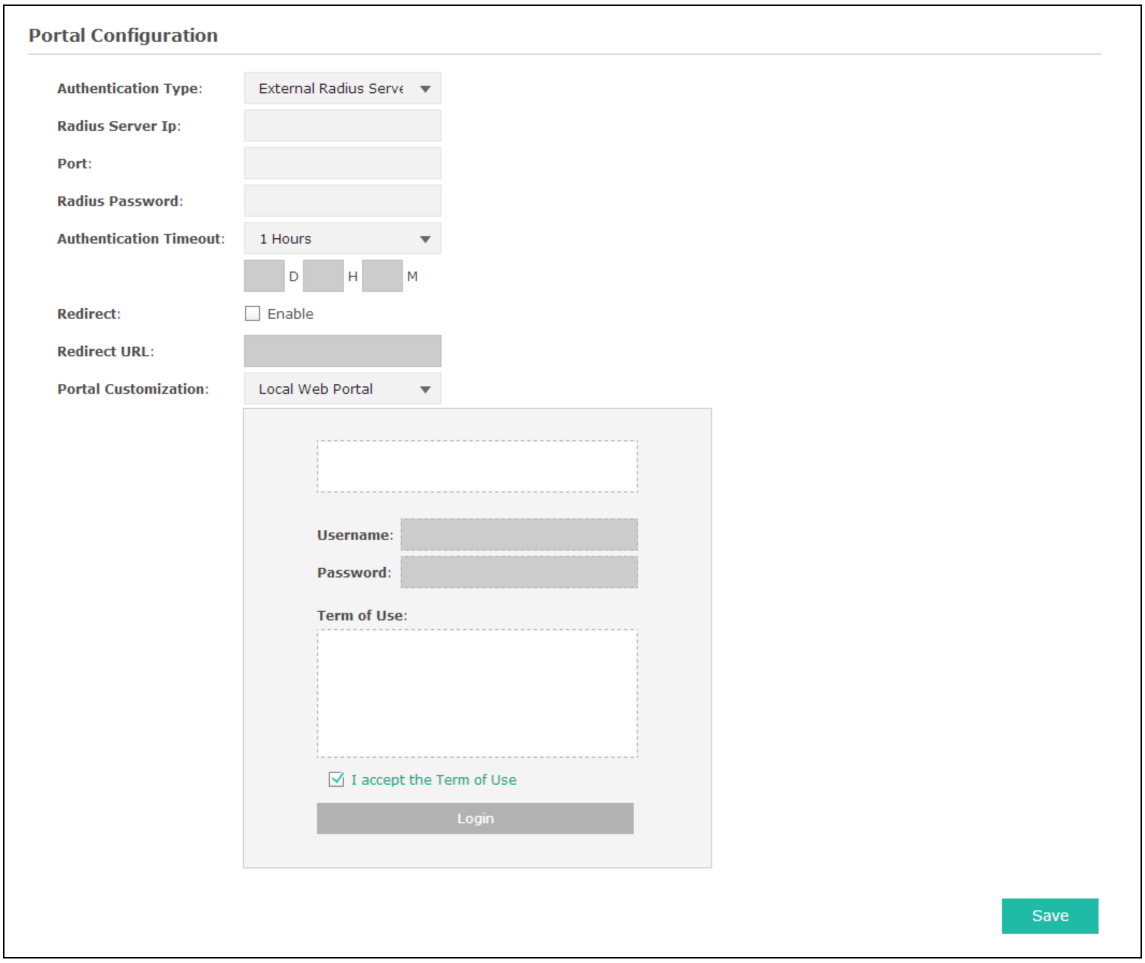
Enter up to 31 characters as the title of the authentication login page in Input Box 1, like “Guest Portal of TP-LINK”.

Enter the terms presented to users in Input Box 2. The terms can be 1 to 1023 characters long.

- ## External RADIUS Server

External RADIUS Server provides 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, as Figure 6-25 shown. The authentication login page of External Web Portal is provided by external portal server, as Figure 6-26 shown.

1. Local Web Portal



Portal Configuration

Authentication Type: External Radius Serve

Radius Server Ip:

Port:

Radius Password:

Authentication Timeout: 1 Hours

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal

Username:

Password:

Term of Use:

☑ I accept the Term of Use

Figure 6-22 Portal Configuration_External RADIUS Server_Local Web Portal

Authentication Type: Select **External RADIUS Server**.

RADIUS Server IP: Enter the IP address of the RADIUS server.

Port: Enter the port for authentication service.

RADIUS Password: Enter the password to log in to the RADIUS server.

Authentication Timeout: After successful verification, an authentication session is established. Authentication Timeout decides the active time of the session. Within active time, the device keeps the authentication session open with the associated client. To reopen the session, the client needs to log in to the web authentication page and enter the user name and password again once authentication timeout is reached.

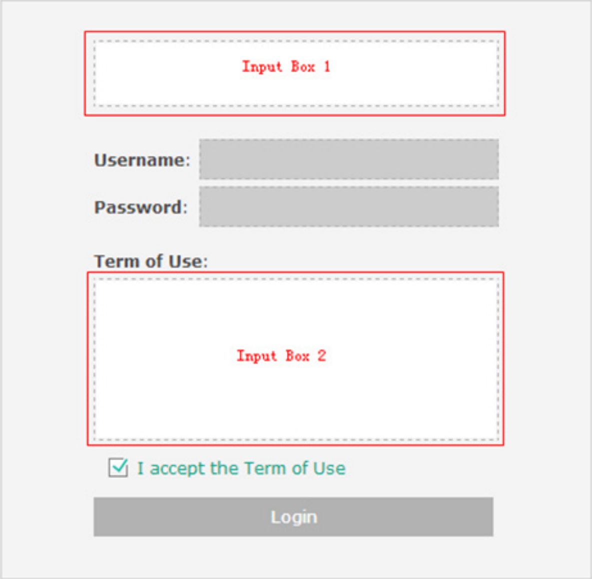
By default, authentication timeout is one hour. Select **Custom** from the drop-down list to customize the parameter.

Redirect: Disable by default. Redirect specifies that the portal should redirect the newly authenticated clients to the configured URL.

Redirect URL: Enter the URL that a newly authenticated client will be directed to.

Portal Customization: Select Local Web Portal, the authentication login page will be provided by the built-in portal server.

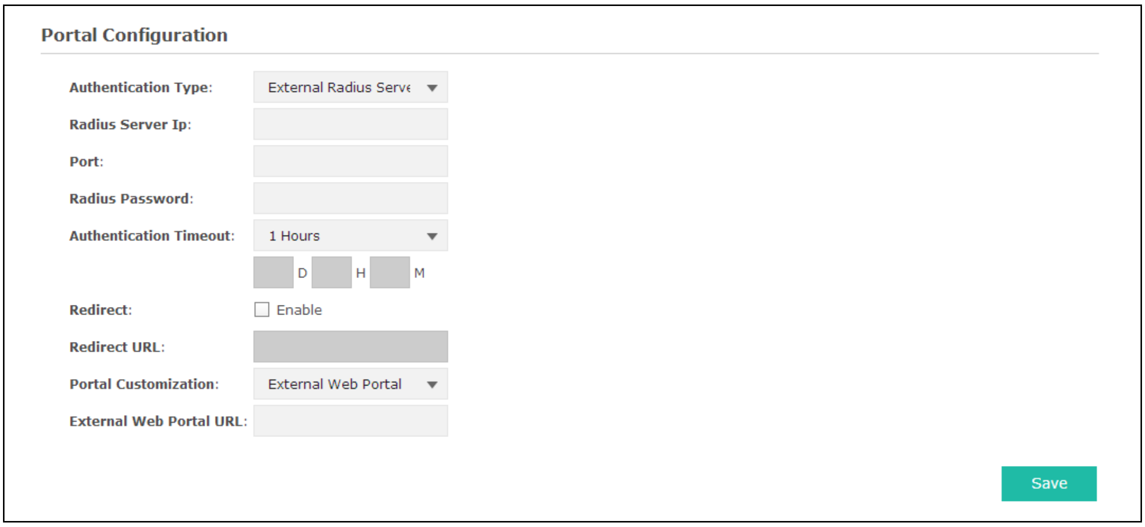
The page below will be presented to users. Words can be filled in Input Box 1 and Input Box 2.



Enter up to 31 characters as the title of the authentication login page in Input Box 1, like “Guest Portal of TP-LINK”.

Enter the terms presented to users in Input Box 2. The terms can be 1 to 1023 characters long.

2. External Web Portal



Portal Configuration

Authentication Type: External Radius Serve

Radius Server Ip:

Port:

Radius Password:

Authentication Timeout: 1 Hours

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: External Web Portal

External Web Portal URL:

Figure 6-23 Portal Configuration_External RADIUS Server_External Web Portal

Authentication Type: Select **External RADIUS Server**.

RADIUS Server IP: Enter the IP address of the RADIUS server.

Port: Enter the port for authentication service.

RADIUS Password: Enter the password to log in to the RADIUS server.

Authentication Timeout: After successful verification, an authentication session is established. Authentication Timeout decides the active time of the session. Within active time, the device keeps the authentication session open with the associated client. To reopen the session, the client needs to log in the web authentication page and enter the user name and password again once authentication timeout is reached.

By default, authentication timeout is one hour. Select **Custom** from the drop-down list to customize the parameter.

Redirect: Disable by default. Redirect specifies that the portal should redirect the newly authenticated clients to the configured URL.

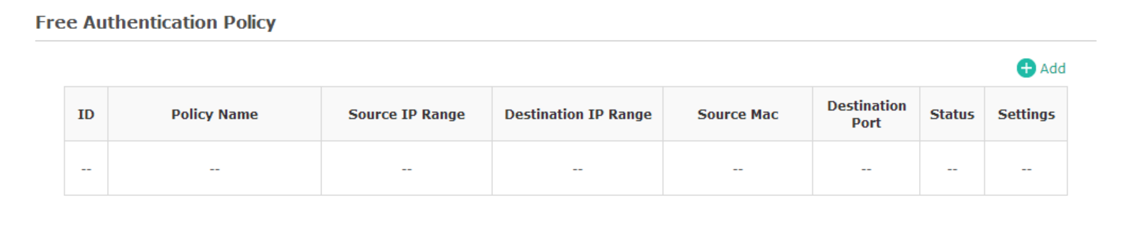
Redirect URL: Enter the URL that a newly authenticated client will be directed to.

Portal Customization: Select **External Web Portal**.

External Web Portal URL: Enter the authentication login page's URL, which is provided by the remote portal server.

6.3.2.2 Free Authentication Policy

Free Authentication Policy allows clients to access network resources for free. On the lower part of the Portal page you can configure and view free authentication policies.

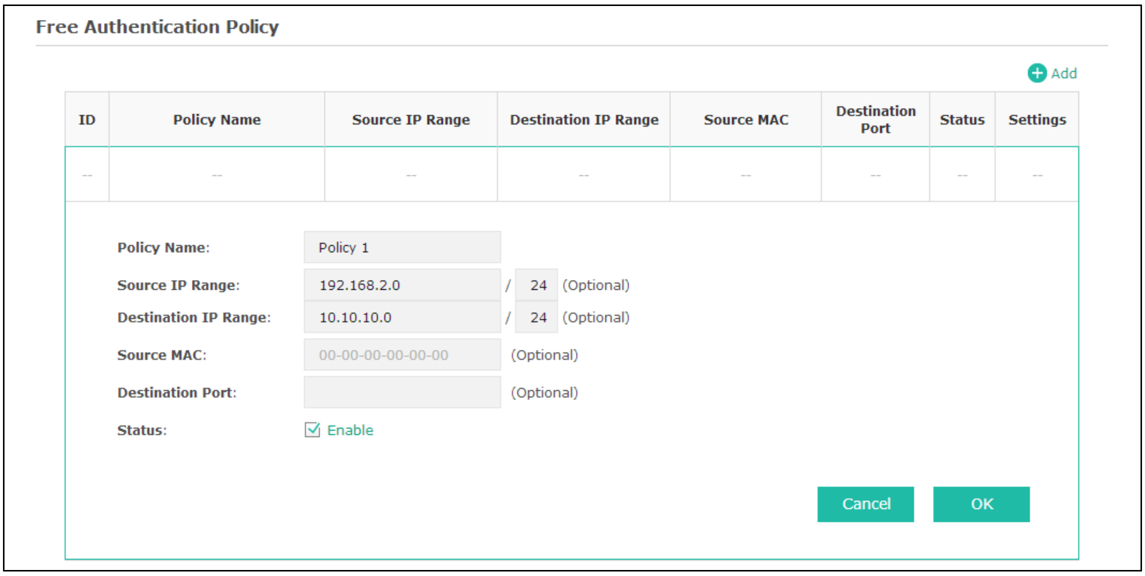


Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source Mac	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Figure 6-24 Free Authentication Policy

Click ⊕ Add to add a new authentication policy and configure its parameters.



Free Authentication Policy

⊕ Add

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Policy Name:	Policy 1
Source IP Range:	192.168.2.0 / 24 (Optional)
Destination IP Range:	10.10.10.0 / 24 (Optional)
Source MAC:	00-00-00-00-00-00 (Optional)
Destination Port:	(Optional)
Status:	☑ Enable

Cancel OK

Figure 6-25 Configure Free Authentication Policy

Policy Name: Enter a policy name.

Source IP Range: Enter the source IP address and subnet mask of the clients who can enjoy the free authentication policy. Leaving the field empty means all IP addresses can access the specific resources.

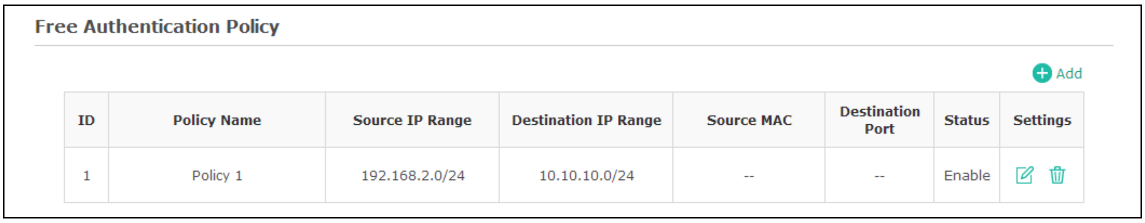
Destination IP Range: Enter the destination IP address and subnet mask for free authentication policy. Leaving the field empty means all IP addresses can be visited.

Source MAC: Enter the source MAC address of the clients who can enjoy the free authentication policy. Leaving the field empty means all MAC addresses can access the specific resources.

Destination Port: Enter the destination port for free authentication policy. Leaving the field empty means all ports can be accessed.

Status: Check the box to enable the policy.

Click the button **OK** in Figure 6-28 and the policy is successfully added as Figure 6-29 shows.



Free Authentication Policy

⊕ Add

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Settings
1	Policy 1	192.168.2.0/24	10.10.10.0/24	--	--	Enable	✎ 🗑

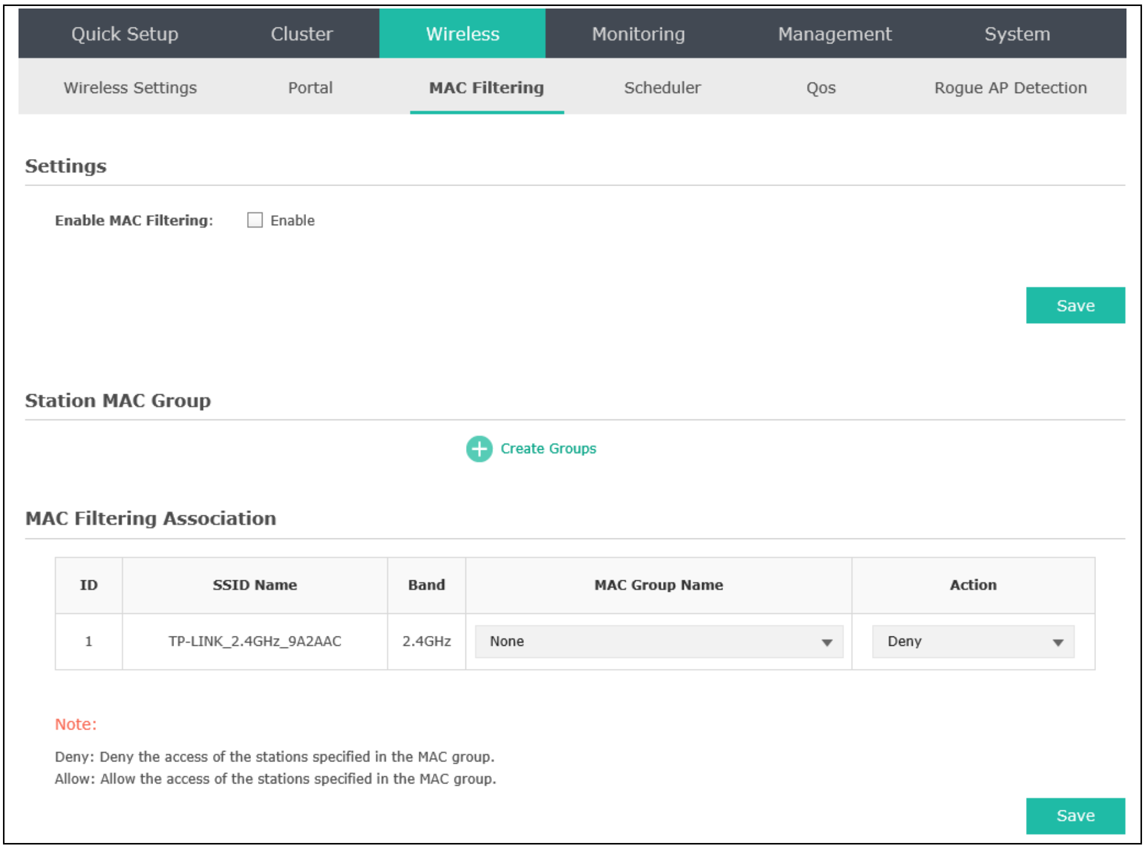
Figure 6-26 Add Free Authentication Policy

Here is the explanation of Figure 6-29: The policy name is Policy 1. Clients with IP address range 192.168.2.0/24 are able to visit IP range 10.10.10.0/24. Policy 1 is enabled.

Click ✎ to edit the policy. Click 🗑 to delete the policy.

6.3.3 MAC Filtering

MAC Filtering uses MAC addresses to determine whether one host can access the wireless network or not. Thereby it can effectively control the user access in the wireless network.



Settings

Enable MAC Filtering: □ Enable

Station MAC Group

MAC Filtering Association

ID	SSID Name	Band	MAC Group Name	Action
1	TP-LINK_2.4GHz_9A2AAC	2.4GHz	None	Deny

Note:

Deny: Deny the access of the stations specified in the MAC group.
Allow: Allow the access of the stations specified in the MAC group.

Figure 6-27 MAC Filtering Page

- ### Settings

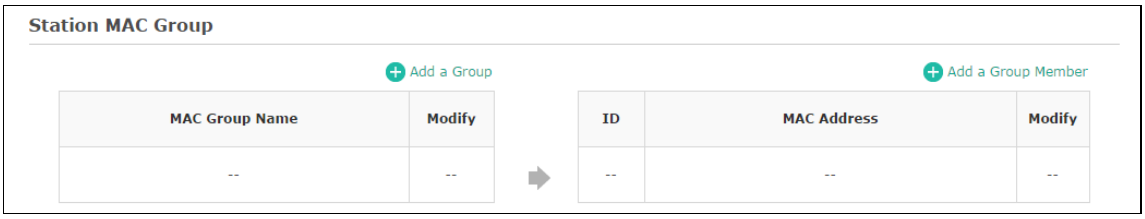
Enable MAC Filtering: Check the box to enable MAC Filtering.

- ### Station MAC Group

Follow the steps below to add MAC groups.

Step 1:

Click ⊕ Create Groups, two tables will be shown.



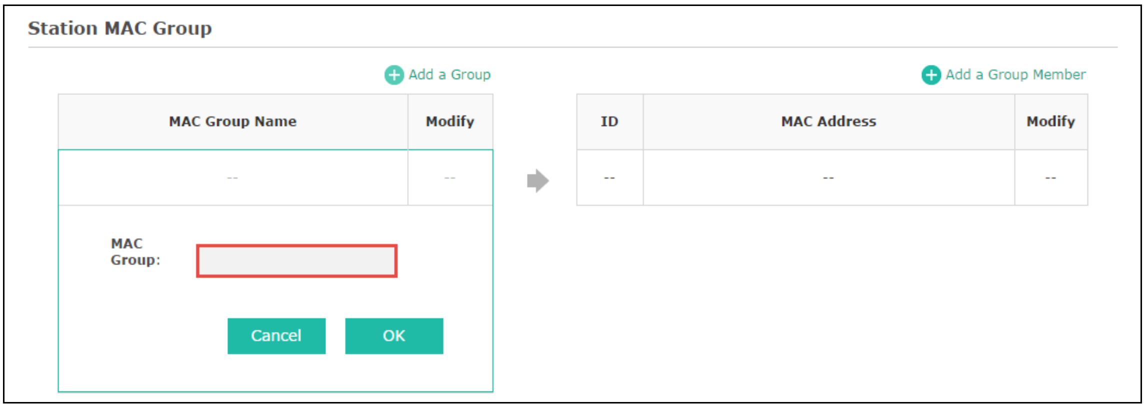
MAC Group Name	Modify
--	--

ID	MAC Address	Modify
--	--	--

Figure 6-28 Station MAC Group

Step 2:

Click + Add a Group and fill in a name for the MAC group.



MAC Group Name	Modify
--	--

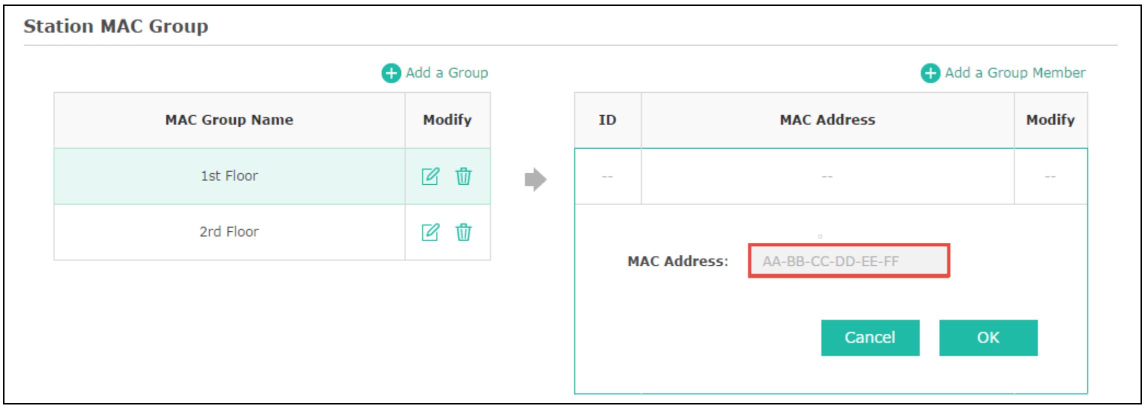
MAC Group:

ID	MAC Address	Modify
--	--	--

Figure 6-29 Add a Group

Step 3:

Click + Add a Group Member and input the MAC address you want to organize into this group.



MAC Group Name	Modify
1st Floor	✎ 🗑
2rd Floor	✎ 🗑

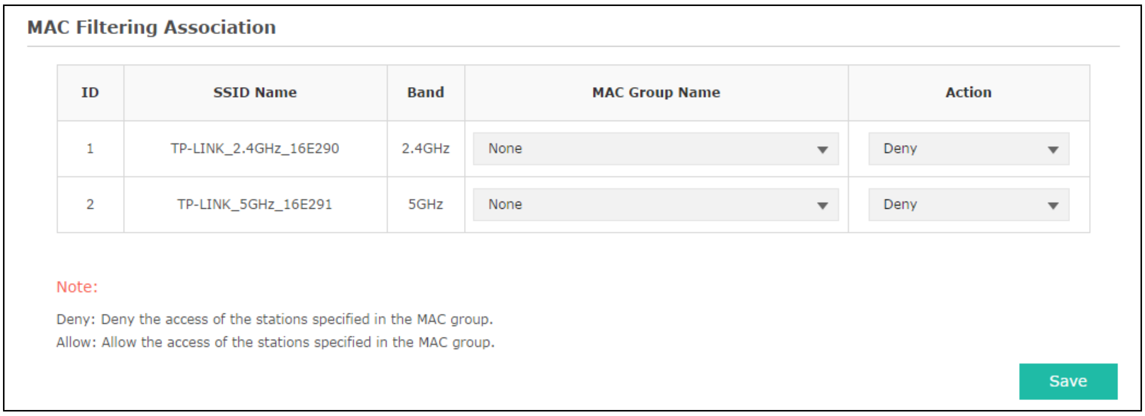
ID	MAC Address	Modify
--	--	--

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

Figure 6-30 Add a Group Member

Click ✎ in Modify column to edit the MAC group name or MAC address. Click 🗑 to delete the MAC group or group member.

- ### MAC Filtering Association



MAC Filtering Association

ID	SSID Name	Band	MAC Group Name	Action
1	TP-LINK_2.4GHz_16E290	2.4GHz	None	Deny
2	TP-LINK_5GHz_16E291	5GHz	None	Deny

Note:

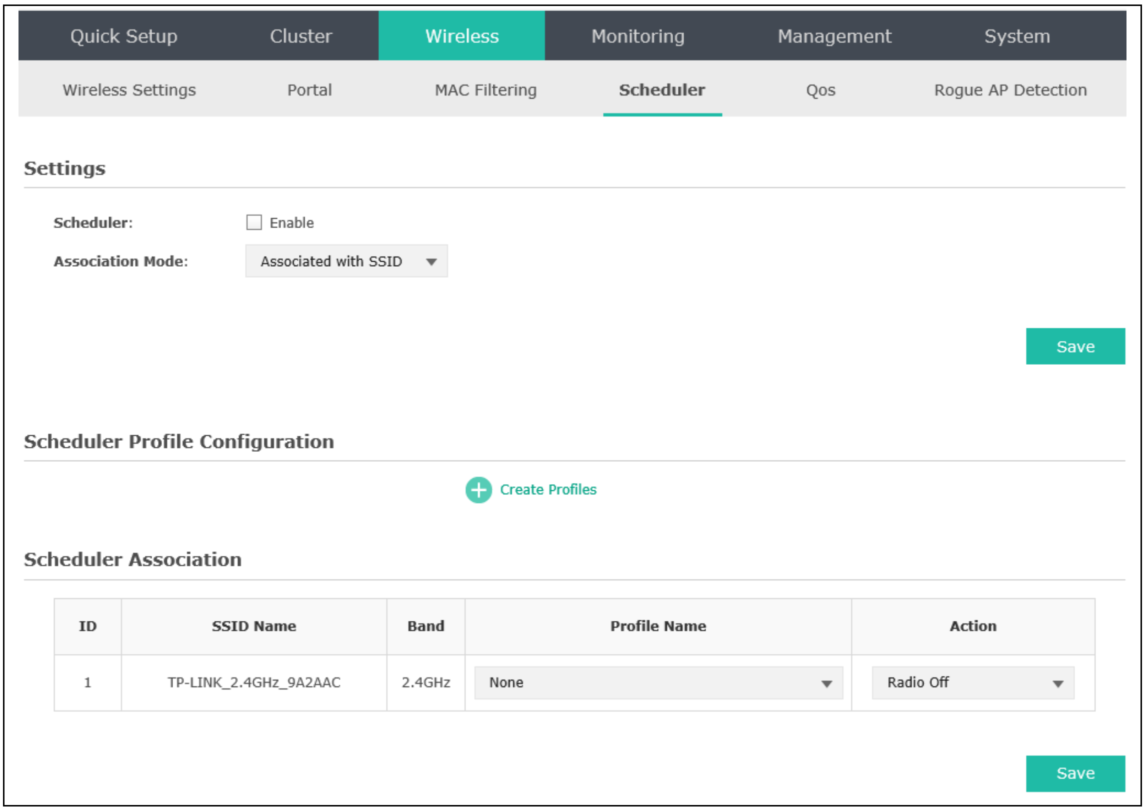
Deny: Deny the access of the stations specified in the MAC group.
Allow: Allow the access of the stations specified in the MAC group.

Figure 6-31 MAC Filtering Association

SSID Name:	Displays the SSID of the wireless network.
Band:	Displays the frequency band the wireless network operates at.
MAC Group Name:	Select a MAC group from the drop-down list to allow or deny its members to access the wireless network.
Action:	• **Allow**: Allow the access of the stations specified in the MAC group. • **Deny**: Deny the access of the stations specified in the MAC group.

6.3.4 Scheduler

Scheduler allows you to configure rules with specific time interval for radios to operate, which automates the enabling or disabling of the radio.



Scheduler: □ Enable

Association Mode: Associated with SSID

ID	SSID Name	Band	Profile Name	Action
1	TP-LINK_2.4GHz_9A2AAC	2.4GHz	None	Radio Off

Figure 6-32 Scheduler Page

- ## Settings

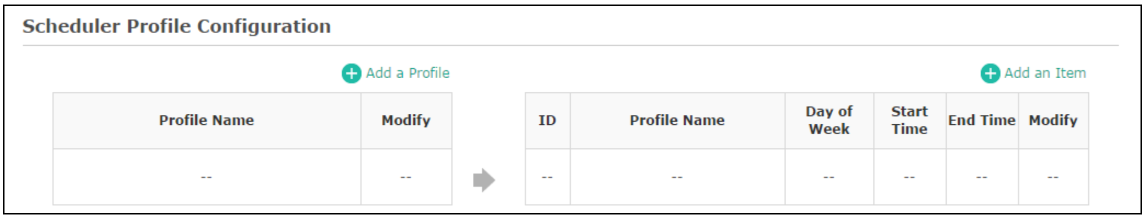
Scheduler:	Check the box to enable Scheduler.
Association Mode:	Select **Associated with SSID/AP**, you can perform configurations on the SSIDs/APs. The display of Scheduler Association is based on your option here.

- ## Scheduler Profile Configuration

Follow the steps below to add rules.

Step 1:

Click ⊕ Create Profiles, two tables will be shown.



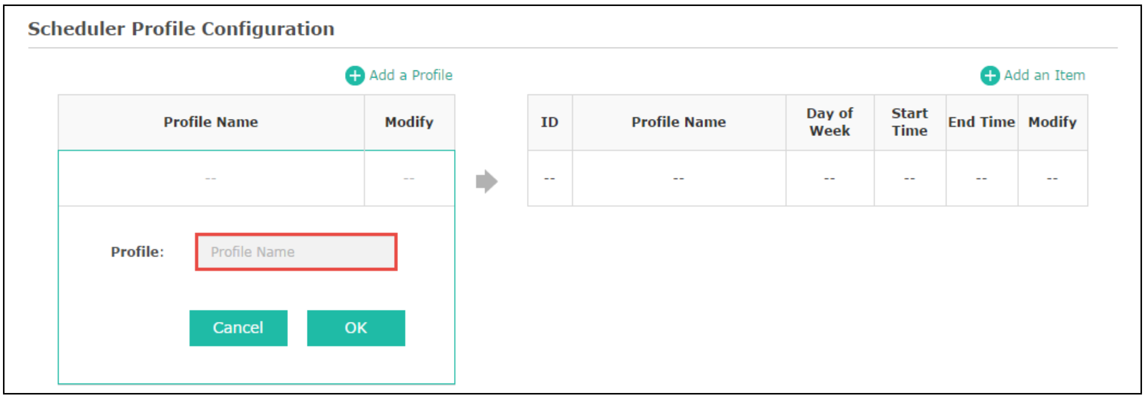
Profile Name	Modify
--	--

ID	Profile Name	Day of Week	Start Time	End Time	Modify
--	--	--	--	--	--

Figure 6-33 Scheduler Profile Configuration

Step 2:

Click ⊕ Add a Profile and input a profile name for the rule.



Scheduler Profile Configuration

⊕ Add a Profile

Profile Name	Modify
--	--

Profile: Profile Name

Cancel OK

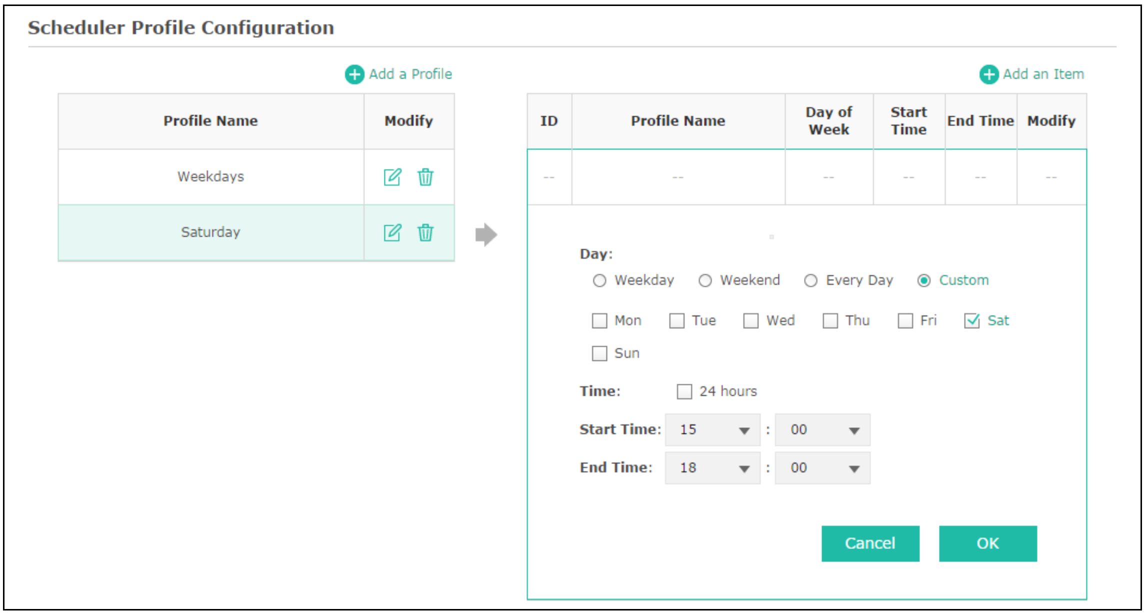
⊕ Add an Item

ID	Profile Name	Day of Week	Start Time	End Time	Modify
--	--	--	--	--	--

Figure 6-34 Add a Profile

Step 3:

Click ⊕ Add a Item and configure the recurring schedule for the rule.



Scheduler Profile Configuration

⊕ Add a Profile

Profile Name	Modify
Weekdays	
Saturday	

⊕ Add an Item

ID	Profile Name	Day of Week	Start Time	End Time	Modify
--	--	--	--	--	--

Day:

○ Weekday ○ Weekend ○ Every Day ● Custom

□ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat

□ Sun

Time: □ 24 hours

Start Time: 15 : 00

End Time: 18 : 00

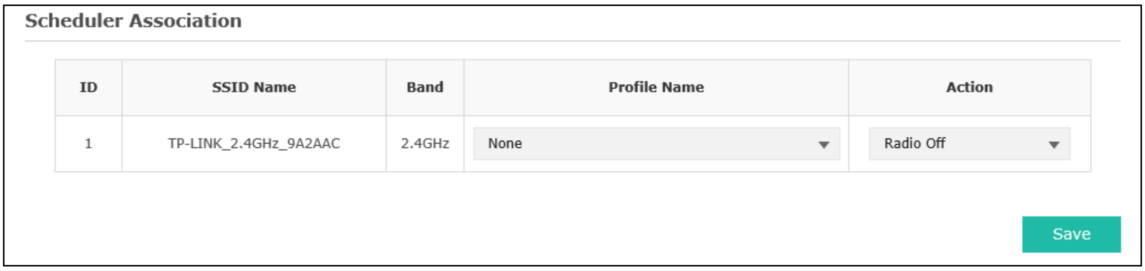
Cancel OK

Figure 6-35 Add a Rule

- ## Scheduler Association

This zone will display different contents based on your selection of association mode in Settings.

1. Associated with SSID



Scheduler Association

ID	SSID Name	Band	Profile Name	Action
1	TP-LINK_2.4GHz_9A2AAC	2.4GHz	None	Radio Off

Figure 6-36 Scheduler Association_Associated with SSID

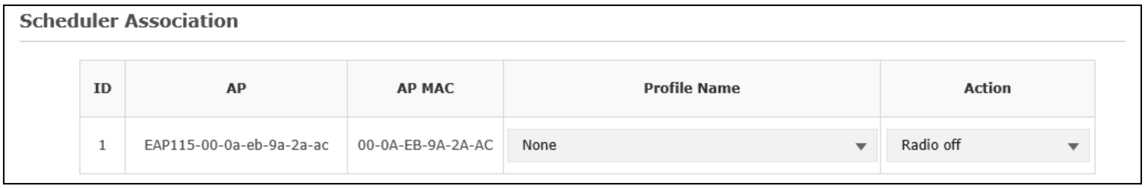
SSID Name: Displays the SSID of an individual device or a cluster.

Band: Displays the frequency band which the wireless network operates at.

Profile Name: Select a profile name from the drop-down list. Profile name is configured in Scheduler Profile Configuration.

Action: Select **Radio On**/**Off** to turn on/off the wireless network during the time interval set for the profile.

2. Associated with AP



Scheduler Association

ID	AP	AP MAC	Profile Name	Action
1	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	None	Radio off

Figure 6-37 Scheduler Association_Associated with AP

AP: Displays the name of the device. If you want to customize the device name, please refer to Device Name.

AP MAC: Displays the MAC address of the device.

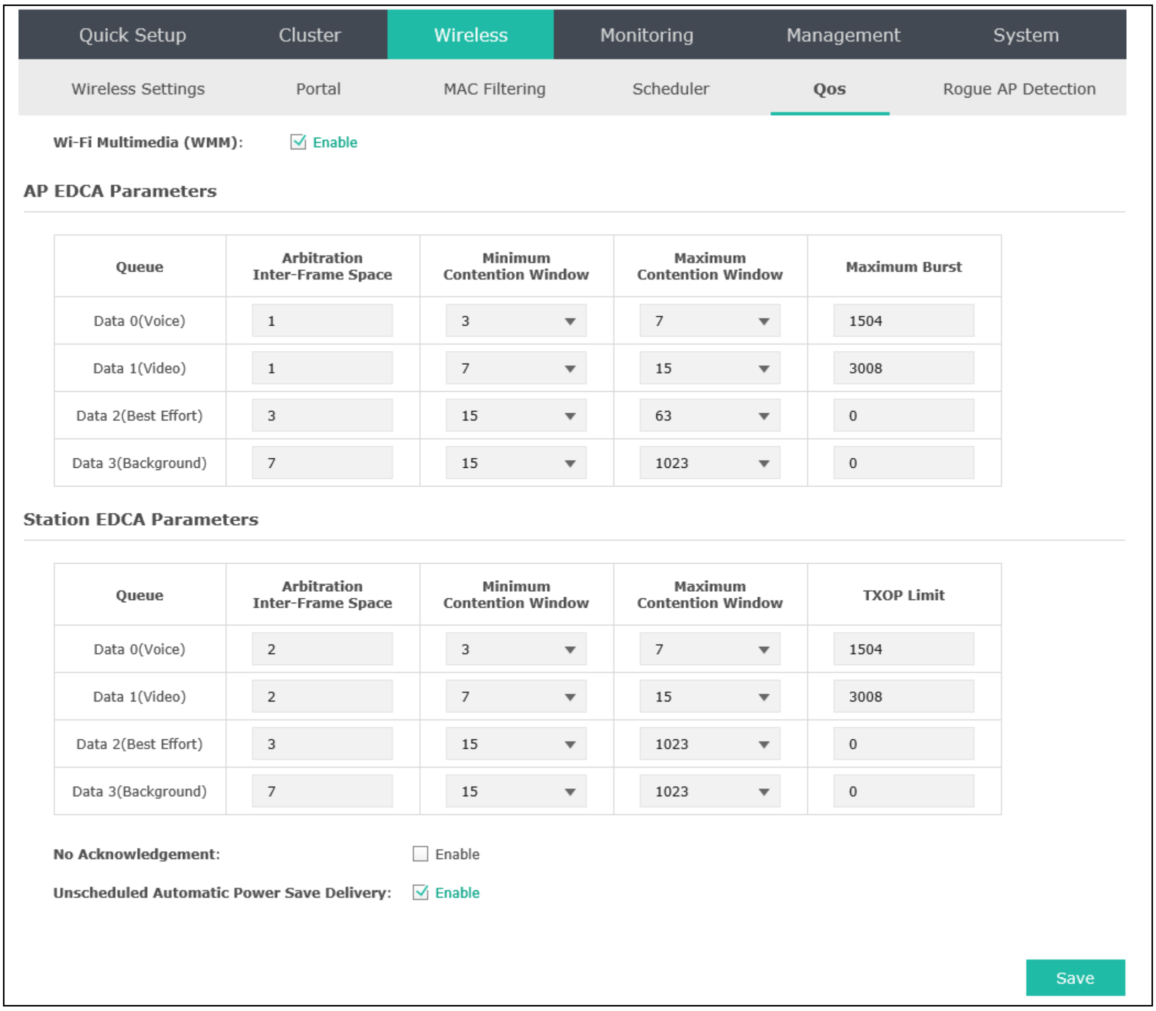
Profile Name: Select a profile name from the drop-down list. Profile name is configured in Scheduler Profile Configuration.

Action: Select **Radio On**/**Off** to turn on/off the wireless network during the time interval set for the profile.

6.3.5 QoS

The EAP supports Quality of Service (QoS) to prioritize voice and video traffic over other traffic types.

In normal use, the default values for the EAP device and station EDCA should not need to be changed. Changing these values affects the QoS provided.



Wi-Fi Multimedia (WMM): ☑ Enable

AP EDCA Parameters

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

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

No Acknowledgement: □ Enable

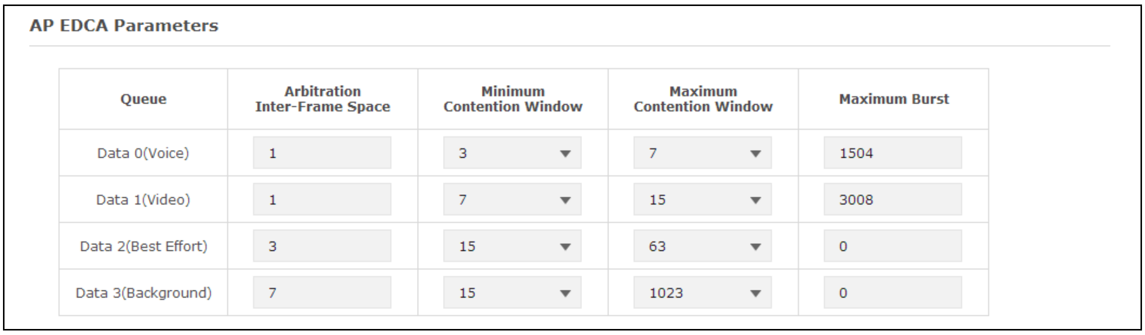
Unscheduled Automatic Power Save Delivery: ☑ Enable

Figure 6-38 QoS Page

Wi-Fi Multimedia (WMM):	By default, WMM is enabled. After WMM is enabled, the device has the QoS function to guarantee the transmission of audio and video packets with high priority.

6.3.5.1 AP EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) parameters affect traffic flowing from the EAP device to the client station.



AP EDCA Parameters

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

Figure 6-39 AP EDCA Parameters

Queue: Displays the transmission queues: Data 0>Data 1>Data 2>Data 3.

Arbitration Inter-Frame Space: A wait time for data frames. The wait time is measured in slots. Valid values for AIFS are from 1 to 15.

Minimum Contention Window: An input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.

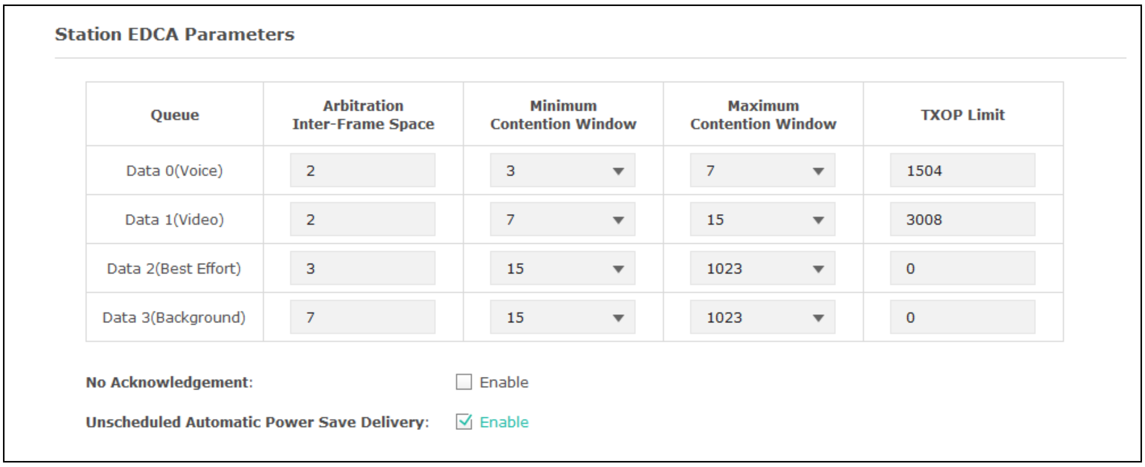
Maximum Contention Window: The upper limit (in milliseconds) for the doubling of the random backoff value.

Maximum Burst This parameter applies only to traffic flowing from EAP to the client station.

This value specifies (in milliseconds) 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. Valid values for Maximum Burst are from 0 to 8192 and should be exactly divided by 32.

6.3.5.2 Station EDCA Parameters

Station EDCA parameters affect traffic flowing from the client station to the EAP device.



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

No Acknowledgement: □ Enable

Unscheduled Automatic Power Save Delivery: ☑ Enable

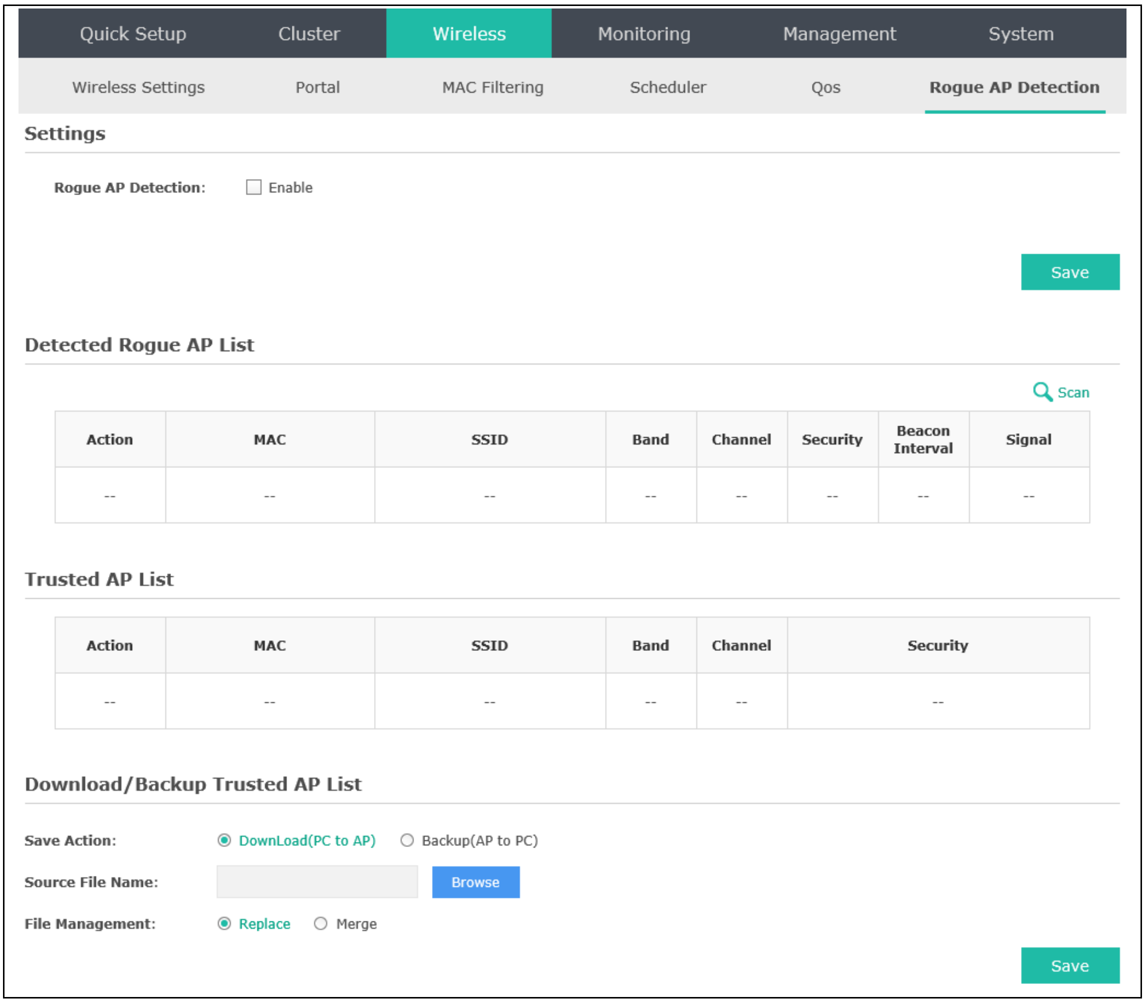
Figure 6-40 Station EDCA Parameters

Queue:	Displays the transmission queues: Data 0>Data 1>Data 2>Data 3.
Arbitration Inter-Frame Space:	A wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 15.
Minimum Contention Window:	An input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.
Maximum Contention Window:	The upper limit (in milliseconds) for the doubling of the random backoff value.
TXOP Limit:	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 towards the EAP device. Valid values for TXOP Limit are from 0 to 8192 and should be exactly divided by 32.
No Acknowledgement:	Select **Enable** to specify that the EAP device should not acknowledge frames with QosNoAck as the service class value. By default, it is disabled.
Unscheduled Automatic Power Save Delivery:	Select **Enable** to enable APSD, which is a power management method. APSD is recommended if VoIP phones access the network through the EAP device. By default, it is enabled.

6.3.6 Rogue AP Detection

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator.

The EAP device can scan all channels to detect all APs in the vicinity of the network. If rogue APs are detected, they are shown on the Detected Rogue AP List. If an AP listed as a rogue is legitimate, you can add it to the Trusted AP List.



Settings

Rogue AP Detection: □ Enable

Detected Rogue AP List

Action	MAC	SSID	Band	Channel	Security	Beacon Interval	Signal
--	--	--	--	--	--	--	--

Trusted AP List

Action	MAC	SSID	Band	Channel	Security
--	--	--	--	--	--

Download/Backup Trusted AP List

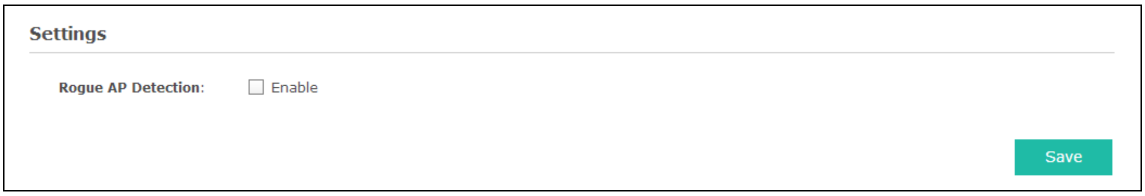
Save Action: ● DownLoad(PC to AP) ○ Backup(AP to PC)

Source File Name:

File Management: ● Replace ○ Merge

Figure 6-41 Rogue AP Detection Page

6.3.6.1 Settings



Settings

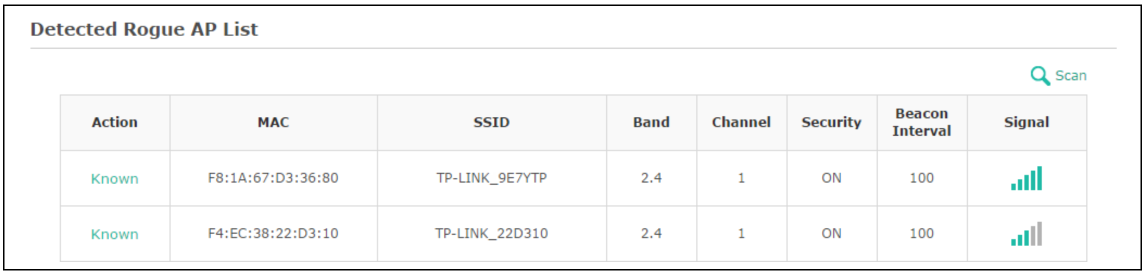
Rogue AP Detection: □ Enable

Figure 6-42 Enable Rogue AP Detection

Rogue AP Detection: Check the box to enable Rogue AP Detection, then click **Save**.

6.3.6.2 Detected Rogue AP List

Information about the detected rogue APs is displayed in the list. By default, the status of the detected rogue AP is unknown. You can click **Known** in Action column to move the AP to the Trusted AP List.



Detected Rogue AP List

Scan

Action	MAC	SSID	Band	Channel	Security	Beacon Interval	Signal
Known	F8:1A:67:D3:36:80	TP-LINK_9E7YTP	2.4	1	ON	100	▂▄▆█
Known	F4:EC:38:22:D3:10	TP-LINK_22D310	2.4	1	ON	100	▂▄▆

Figure 6-43 Detected Rogue AP List

Scan Click to scan rogue APs. Make sure you have enabled Rogue AP Detection and saved the setting before you click the button.

Action: Click **Known** to move the AP to the Trusted AP List. After the configurations are saved, the moved AP will not be displayed in the Detected Rogue AP List.

MAC: The MAC address of the rogue AP.

SSID: The SSID for the rogue AP.

Band: Displays the frequency band which the wireless network of the rogue AP operates at.

Channel: The channel on which the rogue AP is currently broadcasting.

Security: Displays the enabling or disabling of the security mode of the wireless network.

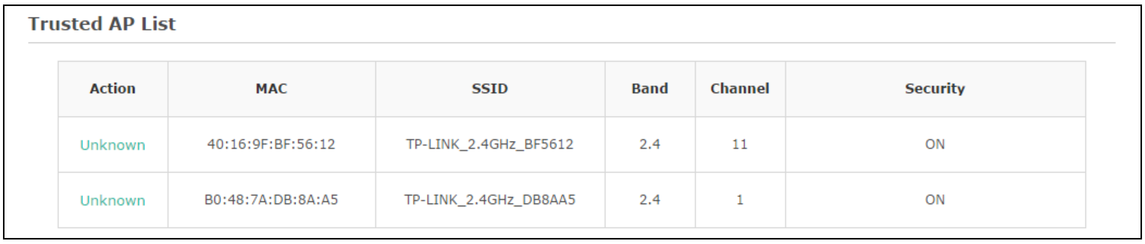
Beacon Interval: The beacon interval used by the rogue AP.

Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

Signal: The strength of the radio signal emitting from the rogue AP.

6.3.6.3 Trusted AP List

Information about the trusted APs is displayed in the list.



Trusted AP List

Action	MAC	SSID	Band	Channel	Security
Unknown	40:16:9F:BF:56:12	TP-LINK_2.4GHz_BF5612	2.4	11	ON
Unknown	B0:48:7A:DB:8A:A5	TP-LINK_2.4GHz_DB8AA5	2.4	1	ON

Figure 6-44 Trusted AP List

Action: Click **Unknown** to move the AP out of the Trusted AP List.

MAC: The MAC address of the trusted AP.

SSID: The SSID for the trusted AP.

Band: Displays the frequency band which the wireless network of the trusted AP operates at.

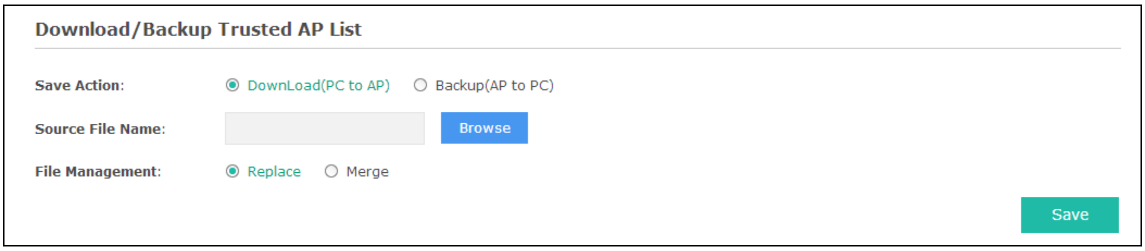
Channel: The channel on which the trusted AP is currently broadcasting.

Security: Displays the enabling or disabling of the security mode of the wireless network.

6.3.6.4 Download/Backup Trusted AP List

You can import a list of trusted APs from a saved list which is acquired from another AP or created from a text file. The AP whose MAC address is in the Trusted AP List will not be detected as a rogue.

You can also backup a list and save it in your PC.



Download/Backup Trusted AP List

Save Action: ● DownLoad(PC to AP) ○ Backup(AP to PC)

Source File Name: Browse

File Management: ● Replace ○ Merge

Save

Figure 6-45 Download/Backup Trusted AP List

Save Action: Select **Download (PC to AP)** to import a trusted AP list to the device.

Select **Backup (AP to PC)** to copy the trusted AP list to your PC.

Source File Name: Click **Browse** and choose the path of a saved trusted AP list or to save a trusted AP list.

File Management: Select **Replace** to import the list and replace the contents of the Trusted AP List.

Select **Merge** to import the list and add the APs in the imported file to the APs currently shown in the Trusted AP List

NOTE:

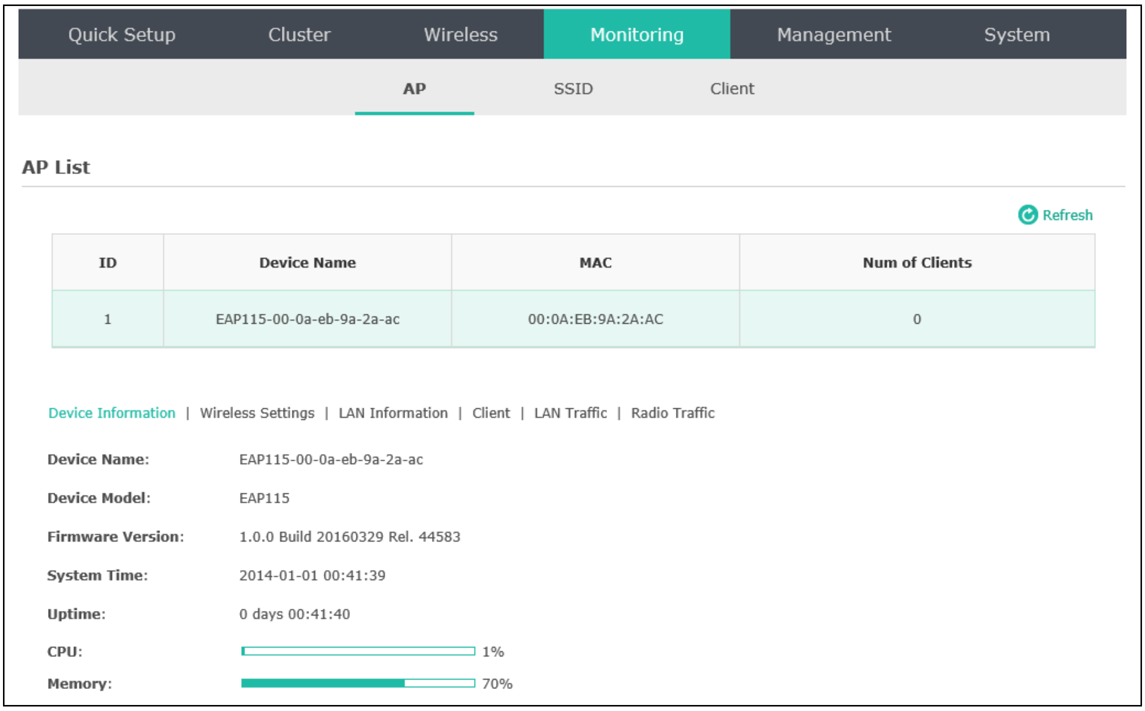
EAP device does not have any control over the APs in the Detected Rogue AP List.

6.4 Monitoring

On Monitoring page, you can monitor the network running status and statistics based on APs, SSIDs and Clients.

6.4.1 AP

AP List on the Monitoring page displays the numbers of EAP devices in a cluster, the MAC address of the EAPs, the number of clients or the corresponding parameters of a standalone AP. Select an AP in the AP List, below which the AP's detailed information will be shown, including Device Information, Wireless Settings, LAN Information, Client, LAN Traffic and Radio Traffic.


Quick Setup
Cluster
Wireless
Monitoring
Management
System
AP
SSID
Client
Refresh
Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

AP List

ID	Device Name	MAC	Num of Clients
1	EAP115-00-0a-eb-9a-2a-ac	00:0A:EB:9A:2A:AC	0

Device Name: EAP115-00-0a-eb-9a-2a-ac

Device Model: EAP115

Firmware Version: 1.0.0 Build 20160329 Rel. 44583

System Time: 2014-01-01 00:41:39

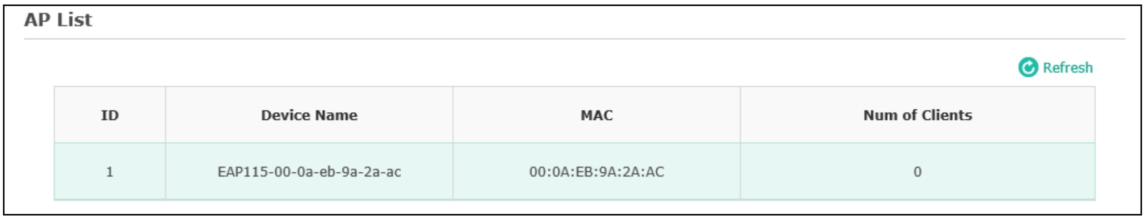
Uptime: 0 days 00:41:40

CPU: 1%

Memory: 70%

Figure 6-46 AP Monitoring

6.4.1.1 AP List



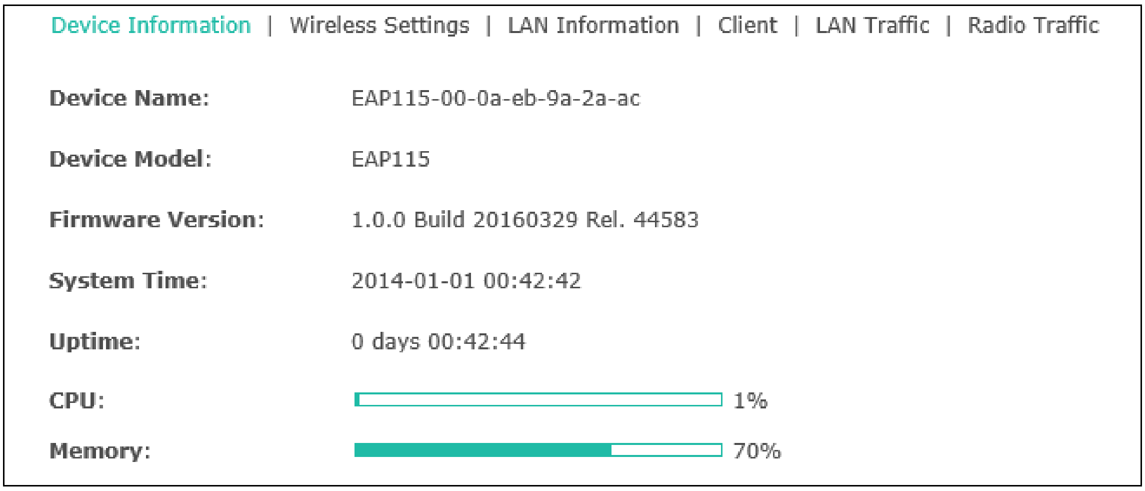
AP List

ID	Device Name	MAC	Num of Clients
1	EAP115-00-0a-eb-9a-2a-ac	00:0A:EB:9A:2A:AC	0

Figure 6-47 AP List

Device Name:	Displays the device name. If you want to customize the device name, please refer to Device Name.
MAC:	Displays the MAC address of the EAP.
Num of Clients:	Displays the number of clients connected to the EAP.

- ## Device Information

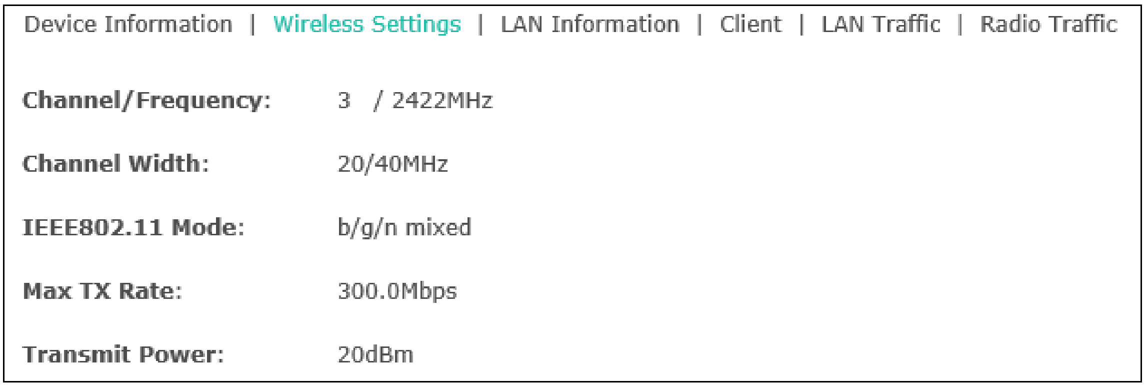

Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Device Name:	EAP115-00-0a-eb-9a-2a-ac
Device Model:	EAP115
Firmware Version:	1.0.0 Build 20160329 Rel. 44583
System Time:	2014-01-01 00:42:42
Uptime:	0 days 00:42:44
CPU:	1%
Memory:	70%

Figure 6-48 Device Information

Device Name:	Displays the device name. If you want to customize the device name, please refer to Device Name.
Device Model:	Displays the model of the device.
Firmware Version:	Displays the firmware version of the device. If you want to upgrade the firmware, please refer to 6.7.5 Firmware Upgrade.
System Time:	Displays the system time of the device. If you want to adjust the system time, please refer to 6.7.2.1 Time Settings.
Uptime:	Displays the time that has elapsed since the last reboot.
CPU:	Displays the CPU occupancy rate, which helps you to preliminarily judge whether the device functions properly.
Memory:	Displays the memory usage rate, which helps you to preliminarily judge whether the device functions properly.

- ## Wireless Settings



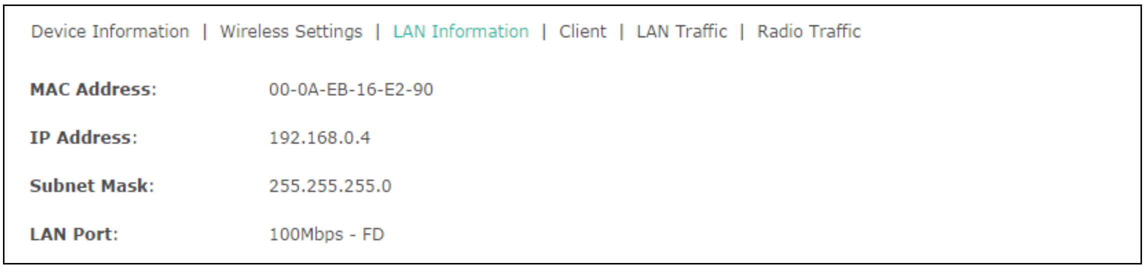
Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Channel/Frequency:	3 / 2422MHz
Channel Width:	20/40MHz
IEEE802.11 Mode:	b/g/n mixed
Max TX Rate:	300.0Mbps
Transmit Power:	20dBm

Figure 6-49 Wireless Settings

Channel/Frequency:	Displays the channel number and the operating frequency. If you want to change them, please refer to Radio in Cluster mode, 6.4.1.1 Wireless Basic Settings in Standalone mode.
Channel Width:	Displays the spectral width of the radio channel used by the device. If you want to change it, refer to Radio in Cluster mode, 6.4.1.1 Wireless Basic Settings in Standalone mode.
IEEE802.11 Mode:	Displays the radio standard used for operation of your device. If you want to change it, refer to Radio in Cluster mode, 6.4.1.1 Wireless Basic Settings in Standalone mode.
Max TX Rate:	Displays the maximum data rate at which the device should transmit wireless packets.
Transmit Power:	Displays the maximum average transmit power of the device. If you want to change it, refer to Radio in Cluster mode, 6.4.1.1 Wireless Basic Settings in Standalone mode.

- ## LAN Information



Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

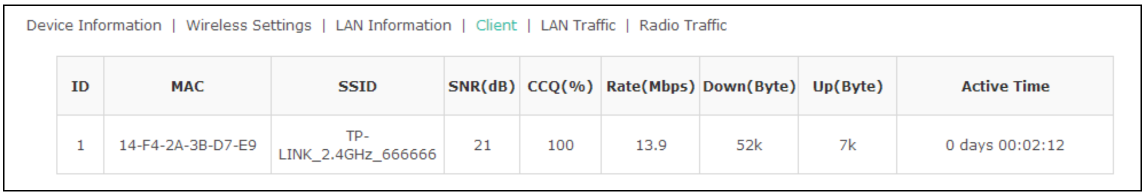
MAC Address:	00-0A-EB-16-E2-90
IP Address:	192.168.0.4
Subnet Mask:	255.255.255.0
LAN Port:	100Mbps - FD

Figure 6-50 LAN Information

MAC Address:	Displays the MAC address of the device.
IP Address:	Displays the IP address of the device.
Subnet Mask:	Displays the subnet mask of the device.

LAN Port: Displays the maximum transmission rate and duplex mode (half-duplex or full-duplex) of the port.

Client


Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

ID	MAC	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time
1	14-F4-2A-3B-D7-E9	TP-LINK_2.4GHz_666666	21	100	13.9	52k	7k	0 days 00:02:12

Figure 6-51 Client

MAC: Displays the MAC address of the client of the AP selected in AP List.

SSID: Displays the SSID the client is connected to.

SNR(dB): Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. The bigger the value of SNR, the better network performance the device provides.

CCQ(%): Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.

Rate(Mbps): Displays the data rate at which the client transmits wireless packets.

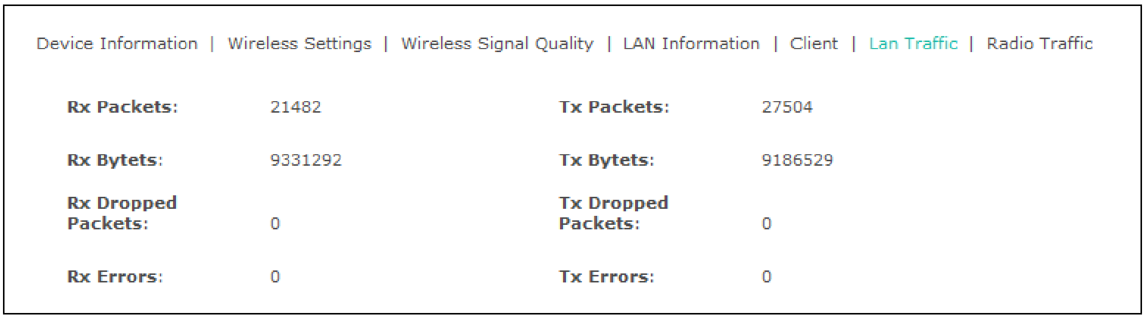
Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

Active Time: Displays the amount of time the client has been connected to the device.

LAN Traffic

Click **LAN Traffic** and you can monitor the data transmission status of the LAN port.


Device Information | Wireless Settings | Wireless Signal Quality | LAN Information | Client | Lan Traffic | Radio Traffic

Rx Packets:	21482	Tx Packets:	27504
Rx Bytets:	9331292	Tx Bytets:	9186529
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

Figure 6-52 LAN Traffic

Rx/Tx Packets: Displays the total amount of packets received/sent on the LAN port.

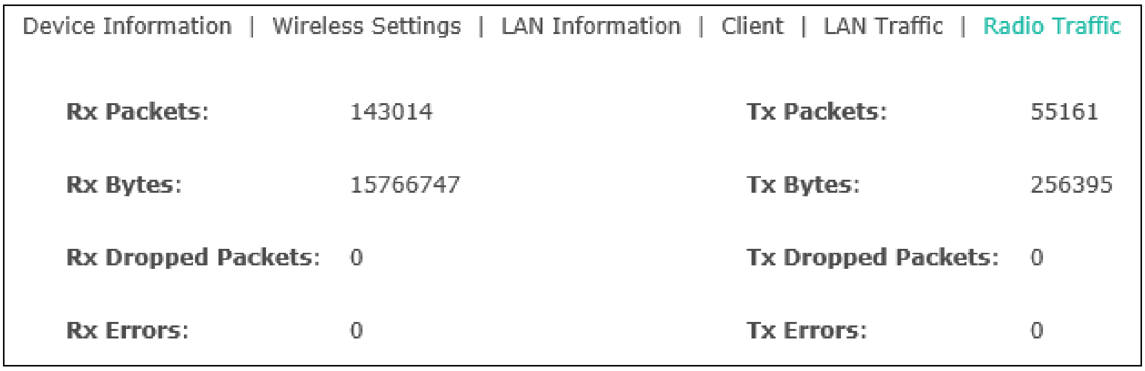
Rx/Tx Bytes: Displays the total amount of data (in bytes) received/sent on the LAN port.

Rx/Tx Dropped Packets: Displays the total amount of dropped packets received/sent on the LAN port.

Rx/Tx Errors: Displays the total amount of error packets received/sent-on the LAN port.

- **Radio Traffic**

Click **Radio Traffic** and you can monitor the data transmission status of the wireless network.



Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Rx Packets:	143014	Tx Packets:	55161
Rx Bytes:	15766747	Tx Bytes:	256395
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

Figure 6-53 Radio Traffic

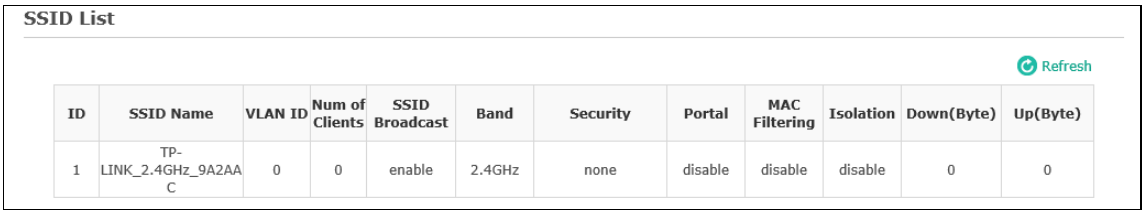
Rx/Tx Packets: Displays the total amount of packets received/sent by the wireless network.

Rx/Tx Bytes: Displays the total amount of data (in bytes) received/sent by the wireless network.

Rx/Tx Dropped Packets: Displays the total amount of dropped packets received/sent by the wireless network.

Rx/Tx Errors: Displays the total amount of error packets received/sent by the wireless network.

6.4.2 SSID



SSID List

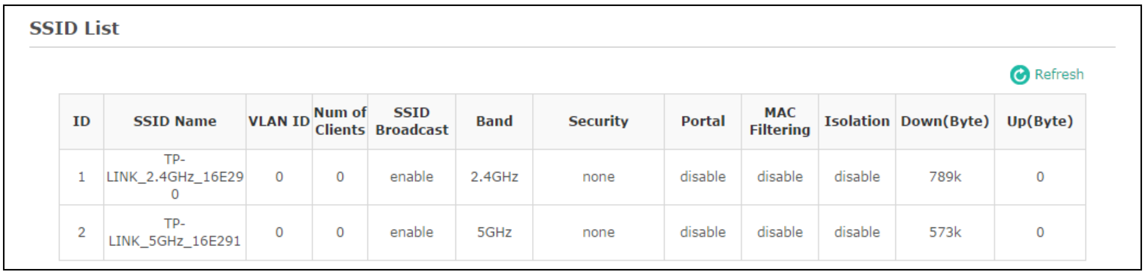
Refresh

ID	SSID Name	VLAN ID	Num of Clients	SSID Broadcast	Band	Security	Portal	MAC Filtering	Isolation	Down(Byte)	Up(Byte)
1	TP-LINK_2.4GHz_9A2AAC	0	0	enable	2.4GHz	none	disable	disable	disable	0	0

Figure 6-54 SSID Monitoring

6.4.2.1 SSID List

In SSID List you can monitor the related parameters of the wireless network.



SSID List

ID	SSID Name	VLAN ID	Num of Clients	SSID Broadcast	Band	Security	Portal	MAC Filtering	Isolation	Down(Byte)	Up(Byte)
1	TP-LINK_2.4GHz_16E290	0	0	enable	2.4GHz	none	disable	disable	disable	789k	0
2	TP-LINK_5GHz_16E291	0	0	enable	5GHz	none	disable	disable	disable	573k	0

Figure 6-55 SSID List

SSID Name: Displays the SSID name. If you want to modify it, please refer to 6.4.1.2 SSIDs.

VLAN ID: Displays the VLAN which the SSID belongs to. If you want to change the VLAN ID, please refer to 6.4.1.2 SSIDs.

Num of Clients: Displays the number of clients connected to the SSID. If you want to get more information about these clients, please refer to 6.4.1.2 SSIDs.

SSID Broadcast: Displays the enabling or disabling of SSID broadcast. If you want to modify it, please refer to 6.4.1.2 SSIDs.

Band: Displays the frequency band the wireless network is operating at.

Security: Displays the security mode the wireless network is applying. If you want to modify it, please refer to6.4.1.2 SSIDs.

Portal: Displays the enabling or disabling of Portal. If you want to modify it, please refer to 6.4.1.2 SSIDs.

MAC Filter: Displays the enabling or disabling of MAC Filtering. If you want to modify it, please refer to 6.4.1.2 SSIDs.

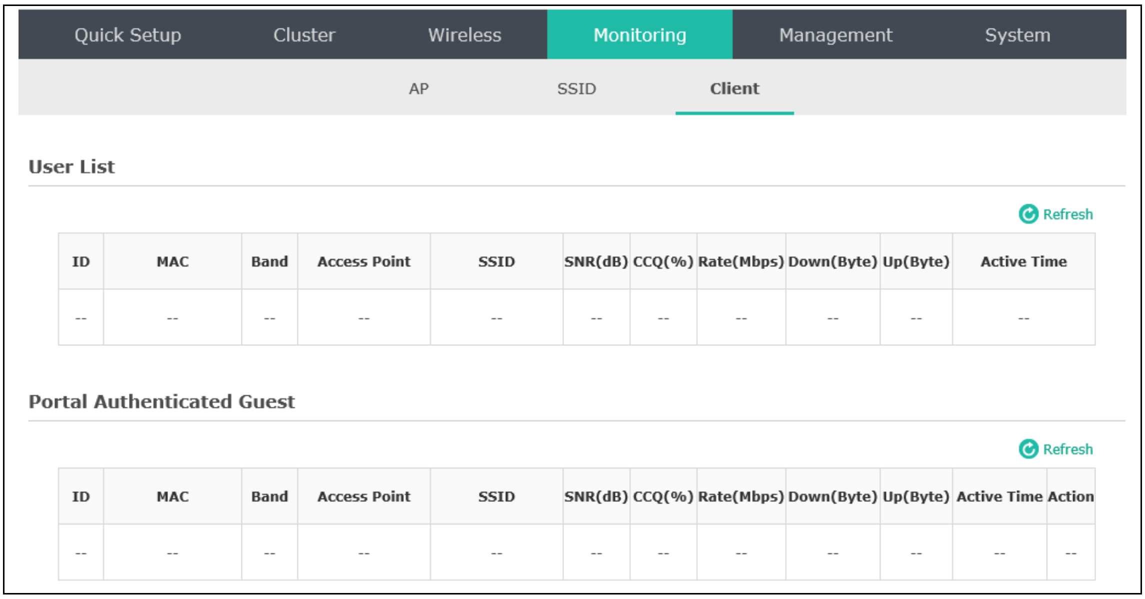
Isolation: Displays the enabling or disabling of SSID Isolation. If you want to modify it, please refer to 6.4.1.2 SSIDs.

Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

6.4.3 Client

From User List, you can monitor the status of all the clients connected to the clustered EAPs including those who are authenticated.



User List

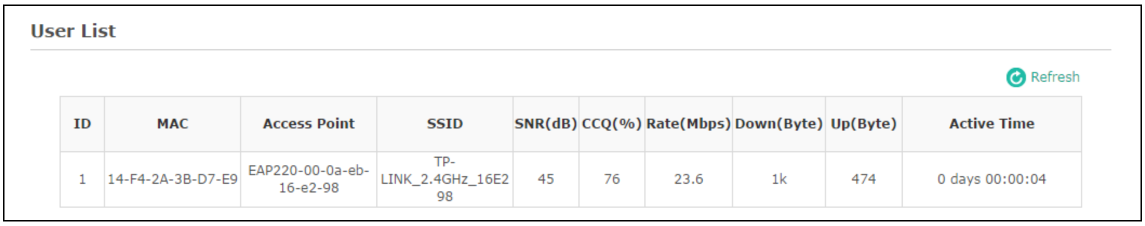
ID	MAC	Band	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time
--	--	--	--	--	--	--	--	--	--	--

Portal Authenticated Guest

ID	MAC	Band	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time	Action
--	--	--	--	--	--	--	--	--	--	--	--

Figure 6-56 Client Monitoring

6.4.3.1 User List



User List

ID	MAC	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time
1	14-F4-2A-3B-D7-E9	EAP220-00-0a-eb-16-e2-98	TP-LINK_2.4GHz_16E298	45	76	23.6	1k	474	0 days 00:00:04

Figure 6-57 User List

MAC: Displays the MAC address of the client.

Access Point: Displays the name of the device to which the client is connected.

SSID: Displays the SSID the client is connected to.

SNR(dB): Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. The bigger the value of SNR, the better network performance the device provides.

CCQ(%): Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.

Rate(Mbps): Displays the data rate at which the client transmits wireless packets.

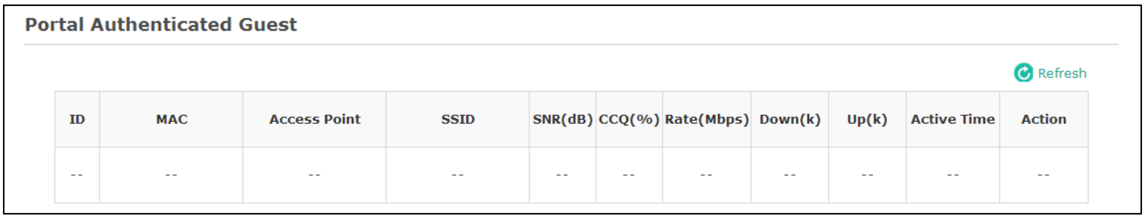
Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

Active Time: Displays the amount of time the client has been connected to the device.

6.4.3.2 Portal Authenticated Guest

The Portal Authenticated Guest displays information about clients that have set up valid authentication.



Portal Authenticated Guest

ID	MAC	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(k)	Up(k)	Active Time	Action
--	--	--	--	--	--	--	--	--	--	--

Figure 6-58 Portal Authenticated Guest

MAC: Displays the MAC address of the authenticated client.

Access Point: Displays the name of the device to which the authenticated client is connected

SSID: Displays the SSID the authenticated client is connected to.

SNR(dB): Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. The bigger the value of SNR, the better network performance the device provides.

CCQ(%): Displays the Client Connection Quality (CCQ) of the authenticated client. CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.

Rate(Mbps): Displays the data rate at which the authenticated client transmits wireless packets.

Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

Active Time: Displays the amount of time the authenticated client has been connected to the root AP.

Action: Click **Unauthorize** to stop giving authorization to the clients connected to the wireless network.

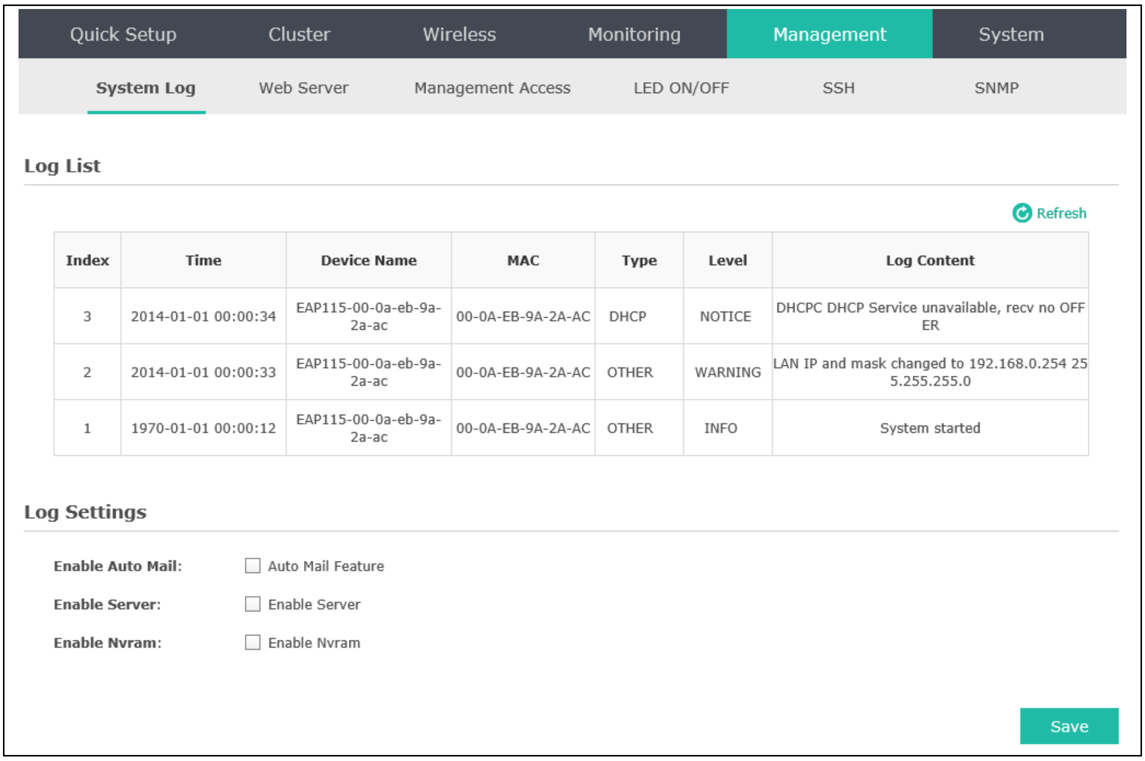
6.5 Management

Management page is mainly used for device management and maintenance.

6.5.1 System Log

System log records information about hardware, software as well as system issues and monitors system events. With the help of system log, you can get informed of system running status and detect the reasons for failure.

Following is the page of System Log.



Log List

Index	Time	Device Name	MAC	Type	Level	Log Content
3	2014-01-01 00:00:34	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	DHCP	NOTICE	DHCPC DHCP Service unavailable, recv no OFFER
2	2014-01-01 00:00:33	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	OTHER	WARNING	LAN IP and mask changed to 192.168.0.254 255.255.255.0
1	1970-01-01 00:00:12	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	OTHER	INFO	System started

Log Settings

Enable Auto Mail: ☐ Auto Mail Feature

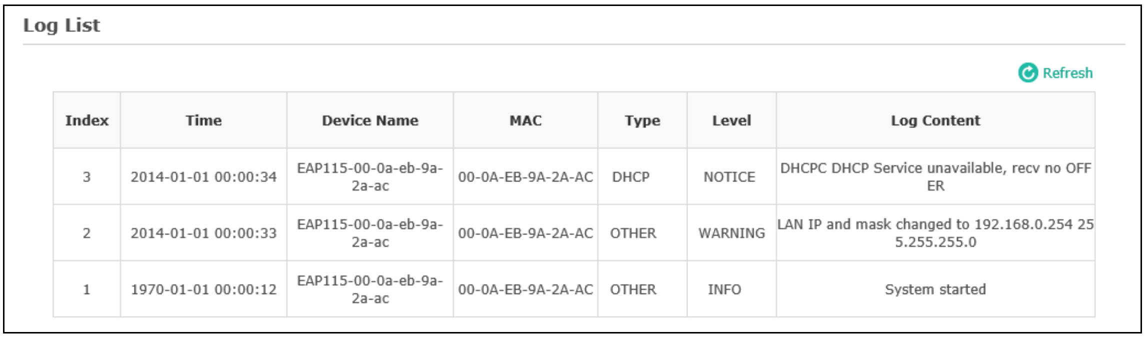
Enable Server: ☐ Enable Server

Enable Nvram: ☐ Enable Nvram

Figure 6-59 System Log Page

6.5.1.1 Log List

From Log List you can view detailed information about hardware, software, system issues and so on.



Log List

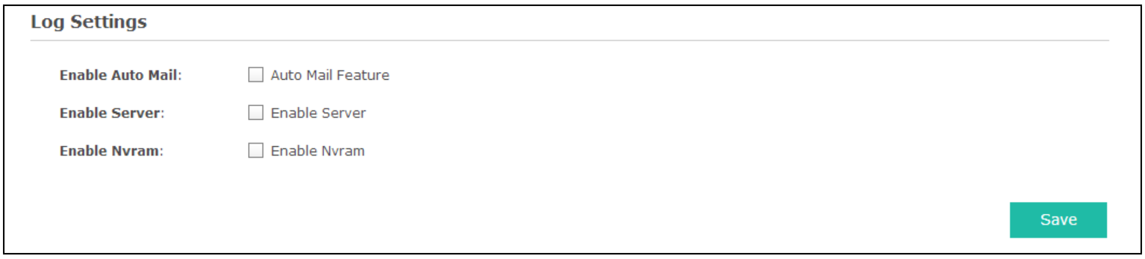
Refresh

Index	Time	Device Name	MAC	Type	Level	Log Content
3	2014-01-01 00:00:34	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	DHCP	NOTICE	DHCPC DHCP Service unavailable, recv no OFFER
2	2014-01-01 00:00:33	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	OTHER	WARNING	LAN IP and mask changed to 192.168.0.254 255.255.255.0
1	1970-01-01 00:00:12	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	OTHER	INFO	System started

Figure 6-60 Log List

6.5.1.2 Log Settings

You can choose the way to receive system logs in Log Settings zone, where these parameters can be configured: Enable Auto Mail, Enable Server and Enable Nvram.



Log Settings

Enable Auto Mail: □ Auto Mail Feature

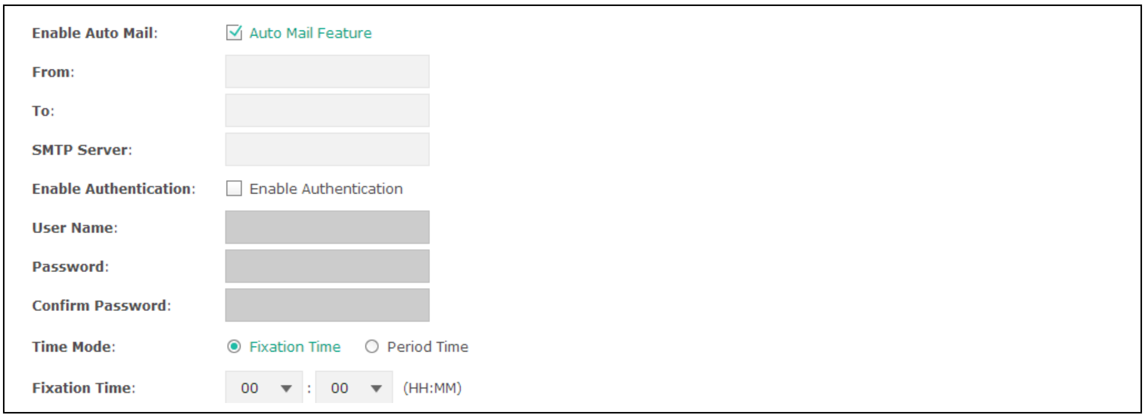
Enable Server: □ Enable Server

Enable Nvram: □ Enable Nvram

Figure 6-61 Log Settings

- **Enable Auto Mail**

If Auto Mail is enabled, system logs will be sent to a mailbox. The following content will be shown.



Enable Auto Mail: ☑ Auto Mail Feature

From:

To:

SMTP Server:

Enable Authentication: □ Enable Authentication

User Name:

Password:

Confirm Password:

Time Mode: ● Fixation Time ○ Period Time

Fixation Time: 00 : 00 (HH:MM)

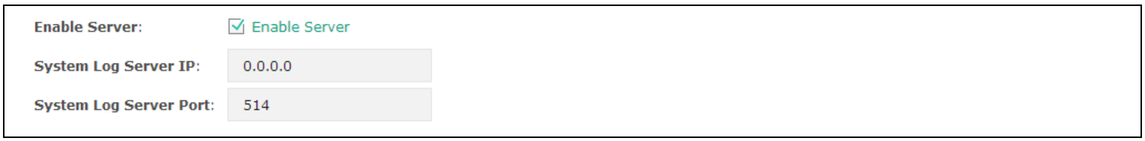
Figure 6-62 Enable Auto Mail

From:	Enter the sender's email address.
To:	Enter the recipient's email address, which will receive the system logs.
SMTP Server:	Enter the IP address of the SMTP server.

Enable Authentication:	Generally users are required to log in to the SMTP server by entering user name and password. • **User Name**: Enter the sender's email address. • **Password**: Enter the password of the sender's email address. • **Confirm Password**: Enter the password again for confirmation.
Time Mode:	System logs can be sent at specific time or time interval. • **Fixation Time**: Set a fixed time, for example, 15:00. The recipient will receive the system logs sent by the device at 15:00 every day. • **Period Time**: Set a time interval, for example, 5 hours. The recipient will receive the system logs sent by the device every 5 hours.

- ## Enable Server

System logs can also be sent to a server. After Auto Mail Feature is enabled, the following content will be shown.



Enable Server: ☑ Enable Server

System Log Server IP: 0.0.0.0

System Log Server Port: 514

Figure 6-63 Enable Server

System Log Server IP:	Enter the IP address of the remote server.
System Log Server Port:	Enter the port of the remote server.

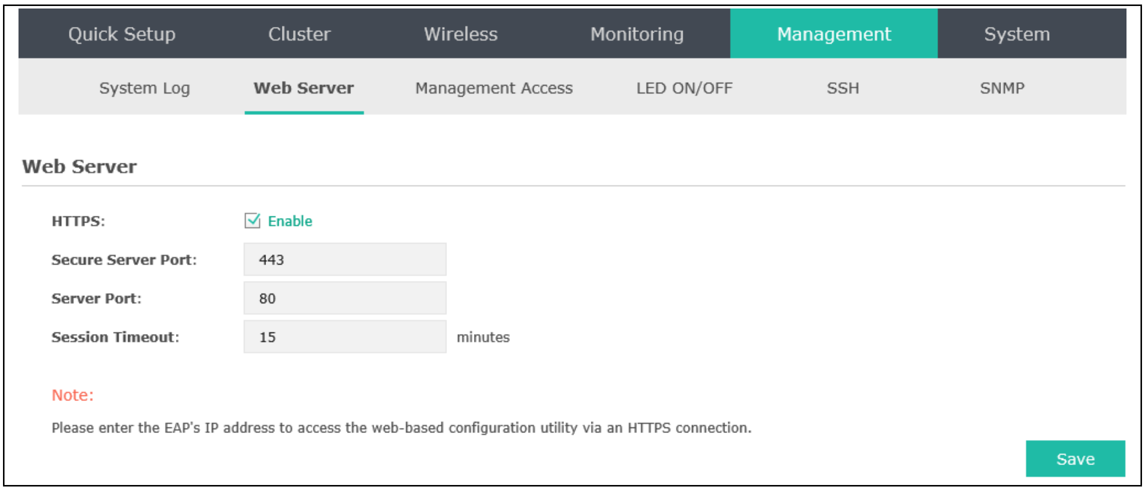
- ## Enable Nvram

By default, Nvram is disabled. Check the box to enable Nvram, system logs will be saved after power supply is cut.

6.5.2 Web Server

You can log in web management interface, thereby manage and maintain the device.

Following is the page of Web Server.



Web Server

HTTPS: ☑ Enable

Secure Server Port: 443

Server Port: 80

Session Timeout: 15 minutes

Note:

Please enter the EAP's IP address to access the web-based configuration utility via an HTTPS connection.

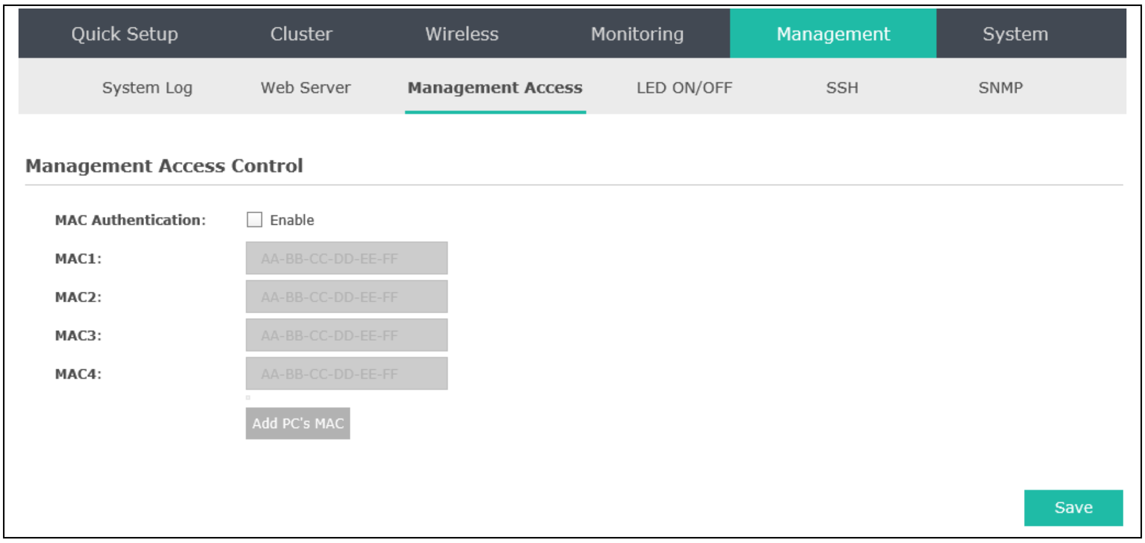
Figure 6-64 Web Server Page

HTTPS:	HTTPS (Hypertext Transfer Protocol Secure) is enabled by default.
Secure Server Port:	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
Server Port:	Designate a server port for web server in HTTP mode. By default the port is 80.
Session Timeout:	Set the session timeout time. If you do nothing with the web management page within the timeout time, the system will log out automatically. Please login again if you want to go back to web management page.

6.5.3 Management Access

Management Access Control allows you to configure up to four MAC addresses of the hosts that are allowed to log in to the web management page of the EAP. Click **Add PC's MAC** and the MAC address of the current host will be added to MAC address list.

Following is the page of Management Access.



Management Access Control

MAC Authentication: □ Enable

MAC1: AA-BB-CC-DD-EE-FF

MAC2: AA-BB-CC-DD-EE-FF

MAC3: AA-BB-CC-DD-EE-FF

MAC4: AA-BB-CC-DD-EE-FF

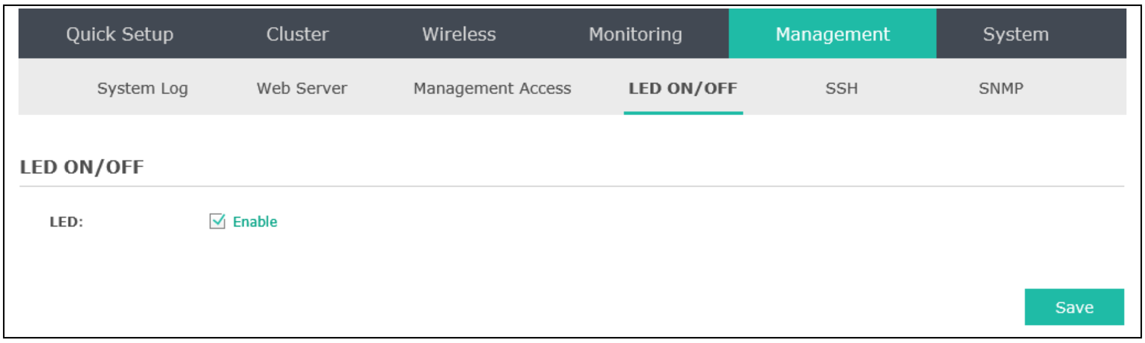
Add PC's MAC

Figure 6-65 Management Access Page

MAC Authentication:	Check the box to enable MAC Authentication. After MAC Authentication is enabled, only the PCs in MAC address list can log in the device's web management page. By default this function is disabled. All PCs in LAN can log in and manage the device.
MAC1~MAC4:	Enter the MAC addresses of the PCs which are authorized to log in the device.

6.5.4 LED ON/OFF

Following is the page of LED ON/OFF. By default the LED is on.



LED ON/OFF

LED: ☑ Enable

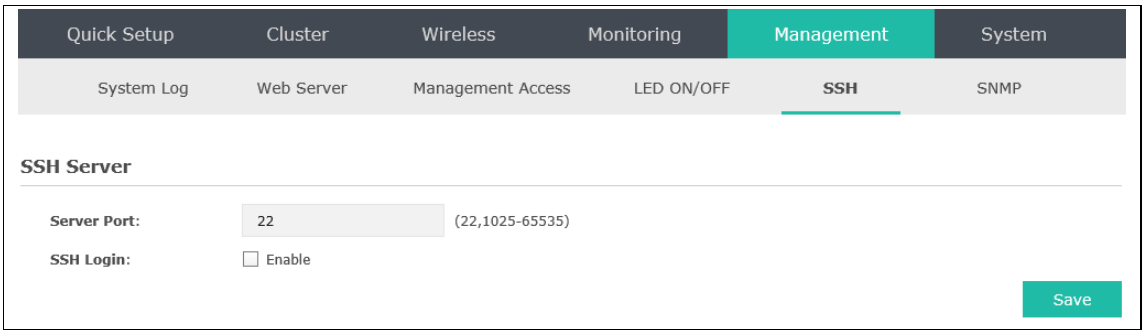
Figure 6-66 LED ON/OFF

6.5.5 SSH

This device supports the SSH Server function that allows users to login and manage it through SSH connection on the SSH client software.

SSH (Secure Shell) is a security protocol established on application and transport layers. SSH-encrypted-connection is similar to a telnet connection, but essentially the old telnet remote management method is not safe, because the password and data transmitted with plain-text can be easily intercepted. SSH can provide information security and powerful authentication when you login this device remotely through an insecure network environment. It can encrypt all the transmission data and prevent the information in remote management from being leaked.

Following is the page of SSH.



SSH Server

Server Port: 22 (22,1025-65535)

SSH Login: □ Enable

Figure 6-67 SSH Page

Server Port:	Enter the server port. By default, it is port 22.
SSH Login:	Check the box to enable SSH Server. By default, it is disabled.

6.5.6 SNMP

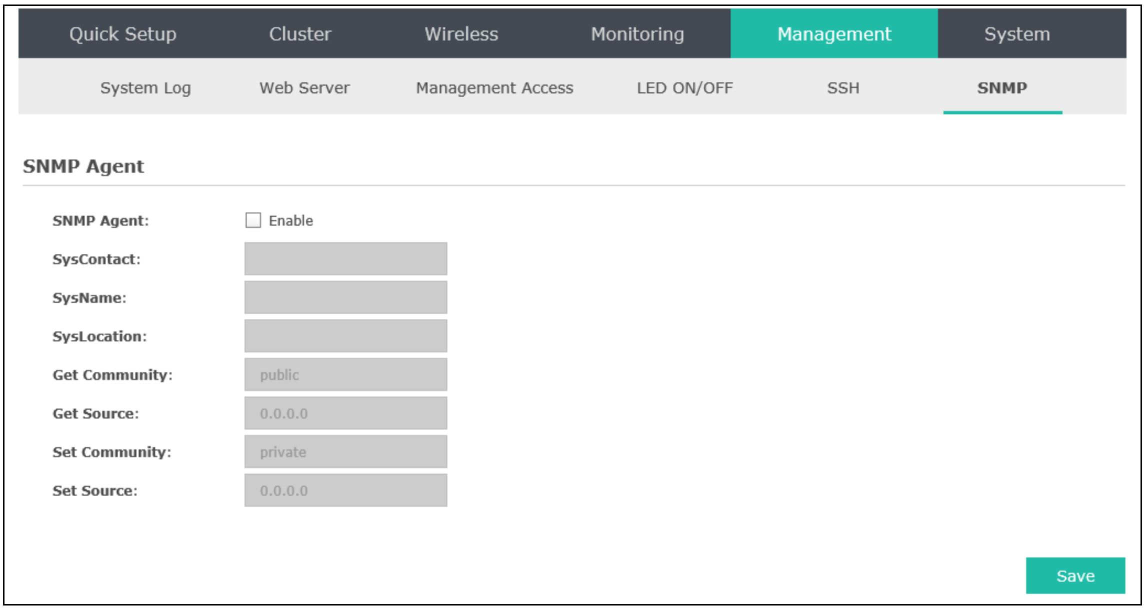
The device can be configured as an SNMP agent.

SNMP (Simple Network Management Protocol), the most widely applied network management protocol, provides a management framework to monitor and maintain Internet devices. Main functions of SNMP include monitoring network performance, detecting and analyzing network error, configuring network devices, and so on. When networks function properly, SNMP can perform the functions of statistics, configuration and testing. When networks have troubles, SNMP can detect and restore these troubles.

An SNMP consists of three key components: manager, agent and MIB (Management Information Base). SNMP manager is a client program operating at workstation, assisting network administrators to accomplish most network device management tasks. An agent is a network-management software module that resides on a managed device and responsible for receiving and dealing with data sent by managing device. Generally the managed devices are network devices including hosts, bridges, switches and routers. MIB is the collection of managed devices. It defines a series of properties of the managed devices. Every SNMP agent has its own MIB.

Once the device has become an SNMP agent, it is able to receive and process request messages from SNMP manager.

Following is the page of SNMP.



SNMP Agent

SNMP Agent: □ Enable

SysContact:

SysName:

SysLocation:

Get Community: public

Get Source: 0.0.0.0

Set Community: private

Set Source: 0.0.0.0

Figure 6-68 SNMP Page

SNMP Agent: Enable SNMP Agent and the SNMP Agent will collect the information of this device and respond to information requests from one or more management systems.

SysContact: Enter the textual identification of the contact person for this managed node.

SysName: Enter an administratively-assigned name for this managed node.

SysLocation: Enter the physical location of this managed node.

Get Community: Community refers to a host group aiming at network management. Get Community only has the read-only right of the device's SNMP information. The community name can be considered a group password. The default setting is public.

Get Source: Defines the IP address (for example, 10.10.10.1) or subnet for management systems that can serve as Get Community to read the SNMP information of this device. The format of subnet is “IP address/bit” (such as 10.10.10.0/24). The default is 0.0.0.0, which means all hosts can read the SNMP information of this device.

Set Community: Set Community has the read and write right of the device's SNMP information. Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered a group password. The default setting is private.

Set Source: Defines the IP address (for example, 10.10.10.1) or subnet for management systems that can serve as Set Community to read and write the SNMP information of this device. The format of subnet is “IP address/bit” (such as 10.10.10.0/24). The default is 0.0.0.0, which means all hosts can read and write the SNMP information of this device.

NOTE:

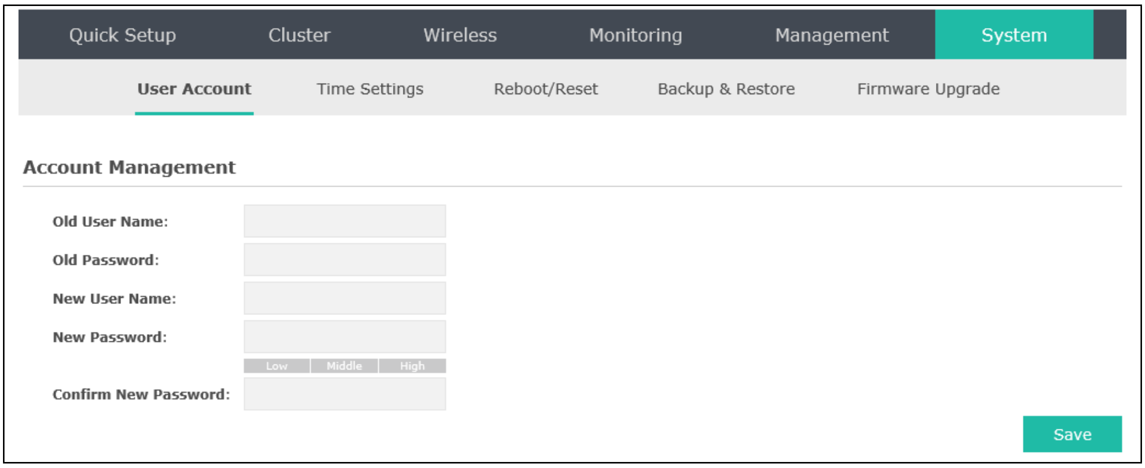
Defining community can allow management systems in the same community to communicate with the SNMP Agent. The community name can be seen as the shared password of the network hosts group. Thus, for the safety, we suggest modifying the default community name before enabling the SNMP Agent service. If the field of community is blank, the SNMP Agent will not respond to any community name.

6.6 System

System page is mainly used to configure some basic information like user account and time, and realize functions including reboot, reset, backup, restore and upgrade the device.

6.6.1 User Account

You can change the user password to protect your device from unauthorized login. We recommend that you change the default user password on the very first system setup.



Account Management

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

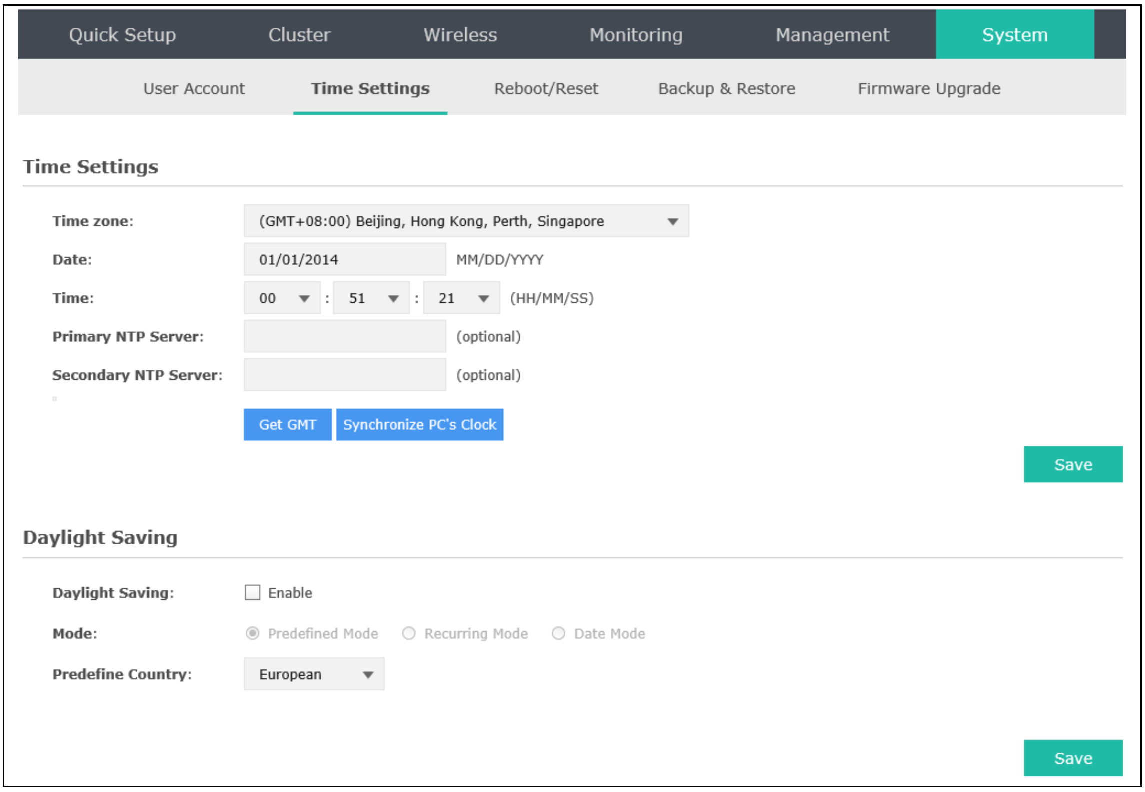
Figure 6-69 User Account Page

Old User Name/Password:	Enter the present user name and password of the admin account to get the permission of modification.
New User Name/Password:	Enter a new user name and password for the admin account. Both values are case-sensitive, up to 64 characters and with no space.
Confirm New Password:	Enter the new password again.

6.6.2 Time Settings

System time represents the device system's notion of the passing of time. System time is the standard time for Scheduler and other time-based functions. You can manually set the system time, configure the system to acquire its time settings from a preconfigured NTP server or synchronize the system time with the PC's clock.

The device supports DST (daylight saving time).



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 01/01/2014 MM/DD/YYYY

Time: 00 : 51 : 21 (HH/MM/SS)

Primary NTP Server: (optional)

Secondary NTP Server: (optional)

Daylight Saving

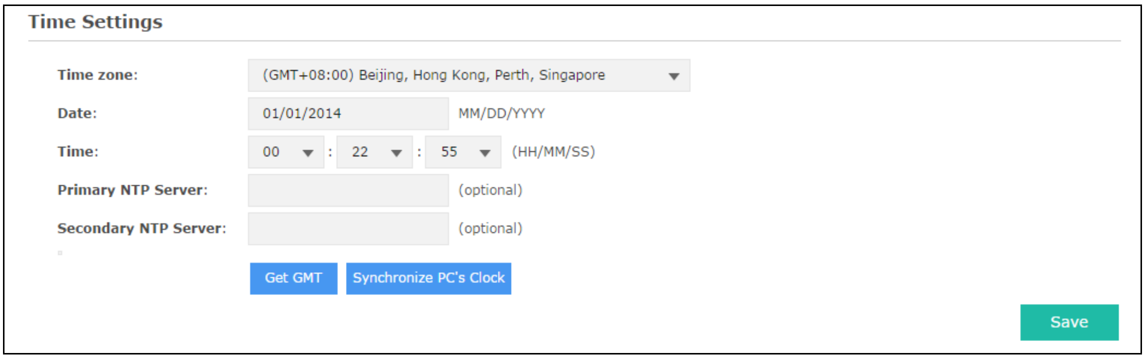
Daylight Saving: □ Enable

Mode: ● Predefined Mode ○ Recurring Mode ○ Date Mode

Predefine Country: European

Figure 6-70 Time Settings

6.6.2.1 Time Settings



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 01/01/2014 MM/DD/YYYY

Time: 00 : 22 : 55 (HH/MM/SS)

Primary NTP Server: (optional)

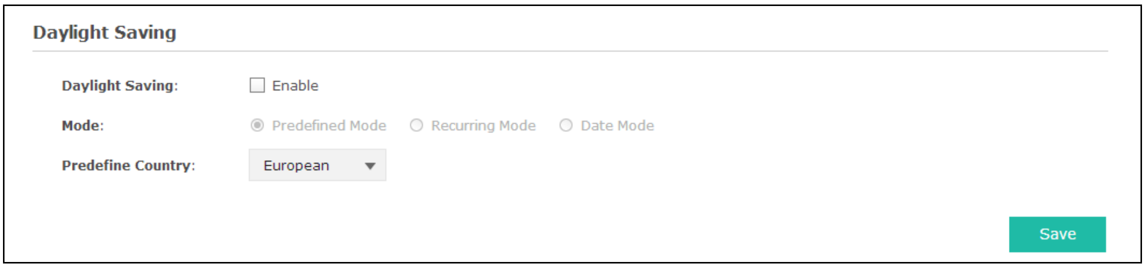
Secondary NTP Server: (optional)

Figure 6-71 Time Settings

Get GMT	Click the button and the device will obtain GMT time from NTP server. IP address of the NTP server has to be filled in.
Synchronize PC's Clock	Click the button, your PC's time will be obtained as the device's system time.
Time zone:	Select your local time zone from the drop-down list.
Date:	Set the current date, in format MM/DD/YYYY. For example, for November 25, 2014, enter 11/25/2014 in the field.

Time:	Specify the device's time. Select the number from the drop-down list in time format HH/MM/SS.
Primary/Secondary NTP Server:	If you've selected **Get GMT** from an NTP server, please input the primary NTP sever address and an alternative NTP server address.

6.6.2.2 Daylight Saving



Daylight Saving

Daylight Saving: □ Enable

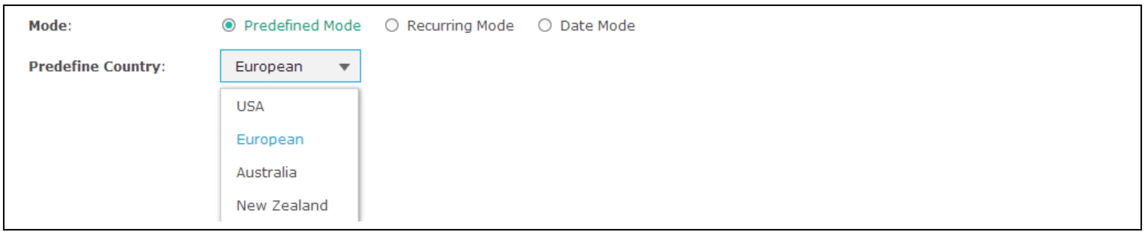
Mode: ● Predefined Mode ○ Recurring Mode ○ Date Mode

Predefine Country: European

Figure 6-72 Daylight Saving

Daylight Saving:	Enable or disable the DST. DST is disabled by default.
Mode:	Options include Predefined Mode, Recurring Mode and Date Mode. Please refer to the following content for more information.

Predefined Mode



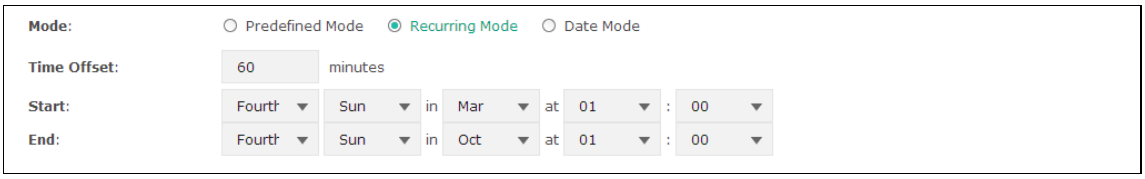
Mode: ● Predefined Mode ○ Recurring Mode ○ Date Mode

Predefine Country: European

Figure 6-73 Predefined Mode

Mode:	Select **Predefined Mode**.
Predefine Country:	Select a predefined DST configuration. Europe is the predefined country by default. • **USA**: Second Sunday in March, 02:00 ~ First Sunday in November, 02:00 • **European**: Last Sunday in March, 01:00 ~ Last Sunday in October, 01:00 • **Australia**: First Sunday in October, 02:00 ~ First Sunday in April, 03:00 • **New Zealand**: Last Sunday in September, 02:00 ~ First Sunday in April, 03:00

- ## Recurring Mode


Mode: ○ Predefined Mode ● Recurring Mode ○ Date Mode

Time Offset: 60 minutes

Start: Fourth Sun in Mar at 01 : 00

End: Fourth Sun in Oct at 01 : 00

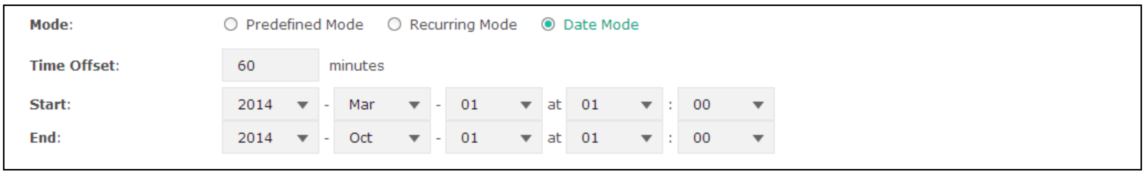
Figure 6-74 Recurring Mode

Mode: Select **Recurring Mode**. The configuration is recurring in use.

Time Offset: Specify the time adding in minutes when Daylight Saving Time comes.

Start/End: Select starting time and ending time of Daylight Saving Time.

- ## Date Mode


Mode: ○ Predefined Mode ○ Recurring Mode ● Date Mode

Time Offset: 60 minutes

Start: 2014 - Mar - 01 at 01 : 00

End: 2014 - Oct - 01 at 01 : 00

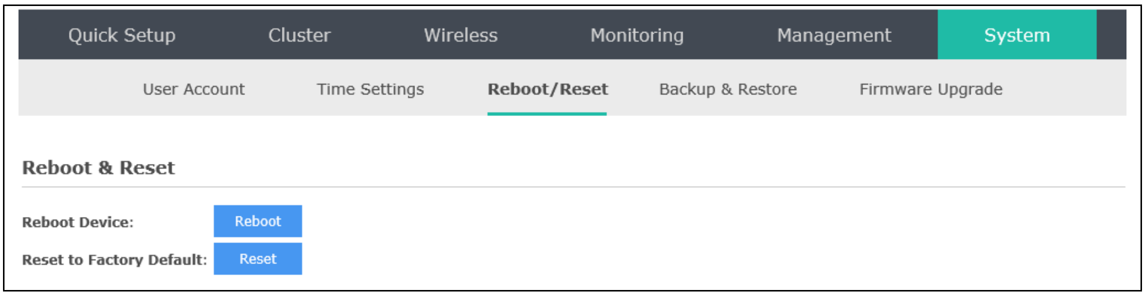
Figure 6-75 Date Mode

Mode: Select **Date Mode**.

Time Offset: Specify the time adding in minutes when Daylight Saving Time comes.

Start/End: Select starting time and ending time of Daylight Saving Time.

6.6.3 Reboot/Reset



Reboot & Reset

Reboot Device: Reboot

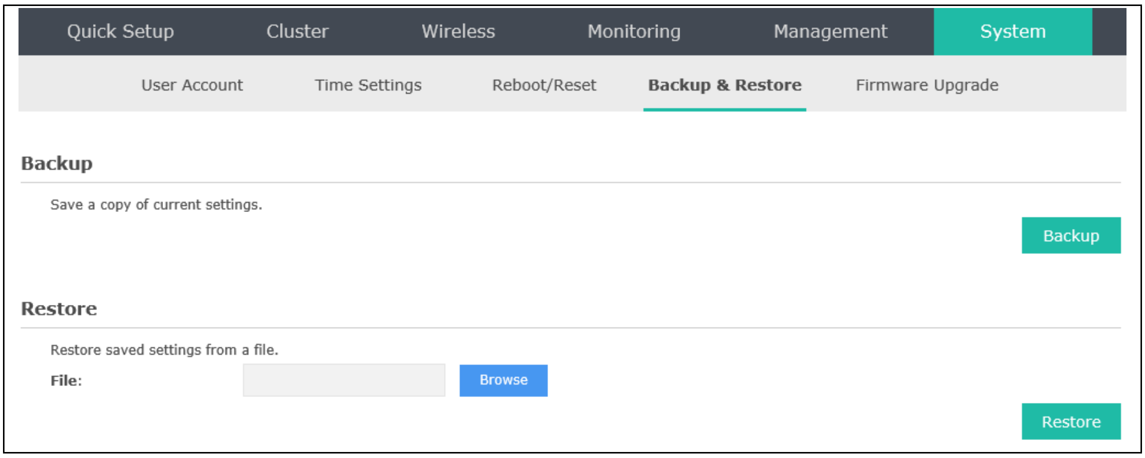
Reset to Factory Default: Reset

Figure 6-76 Reboot & Reset

Click **Reboot** to restart the device. Click **Reset** to restore the device to factory default settings.

> ***NOTE:***
>
> Clicking **Reboot**/**Reset** will reboot/reset all the EAPs in a cluster.

6.6.4 Backup & Restore



Backup

Save a copy of current settings.

Restore

Restore saved settings from a file.

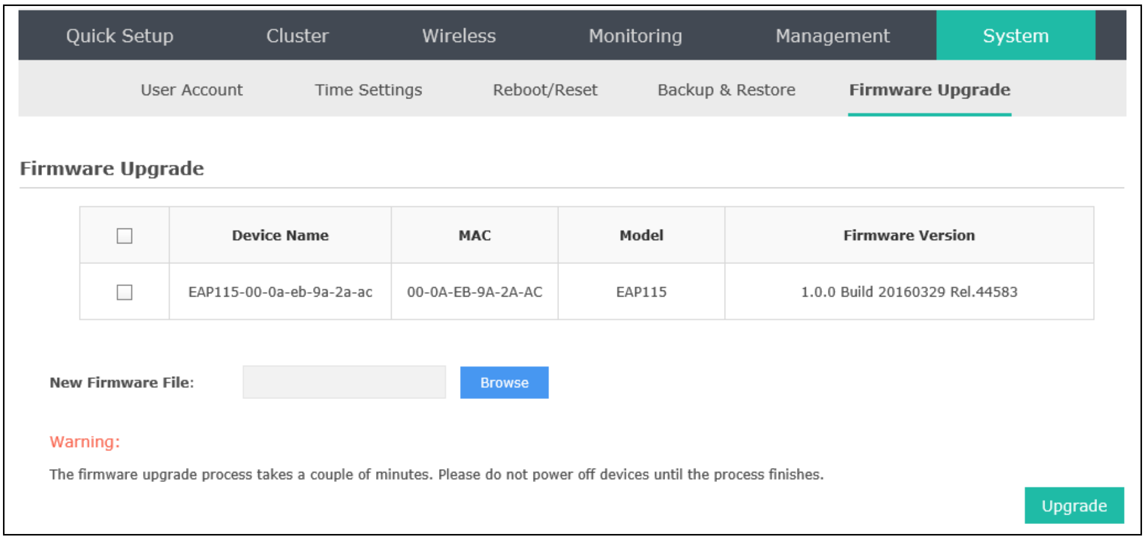
File:

Figure 6-77 Backup & Restore

You can save the current configuration of the EAP as a backup file and restore the configuration via a backup file. Back up the settings before you upgrade the device or upload a new configuration file can prevent it from being lost.

Restore function helps you to restore the device to previous settings by uploading a backup file.

6.6.5 Firmware Upgrade



Firmware Upgrade

□	Device Name	MAC	Model	Firmware Version
□	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	EAP115	1.0.0 Build 20160329 Rel.44583

New Firmware File:

Warning:

The firmware upgrade process takes a couple of minutes. Please do not power off devices until the process finishes.

Figure 6-78 Firmware Upgrade

Please log in http://www.tp-link.com/en/ to download the latest system file. As Figure 6-81 shows, firstly select the model and device you are planning to upgrade. Then click **Browse** and choose the firmware file. Finally click **Upgrade** to upgrade the devices.

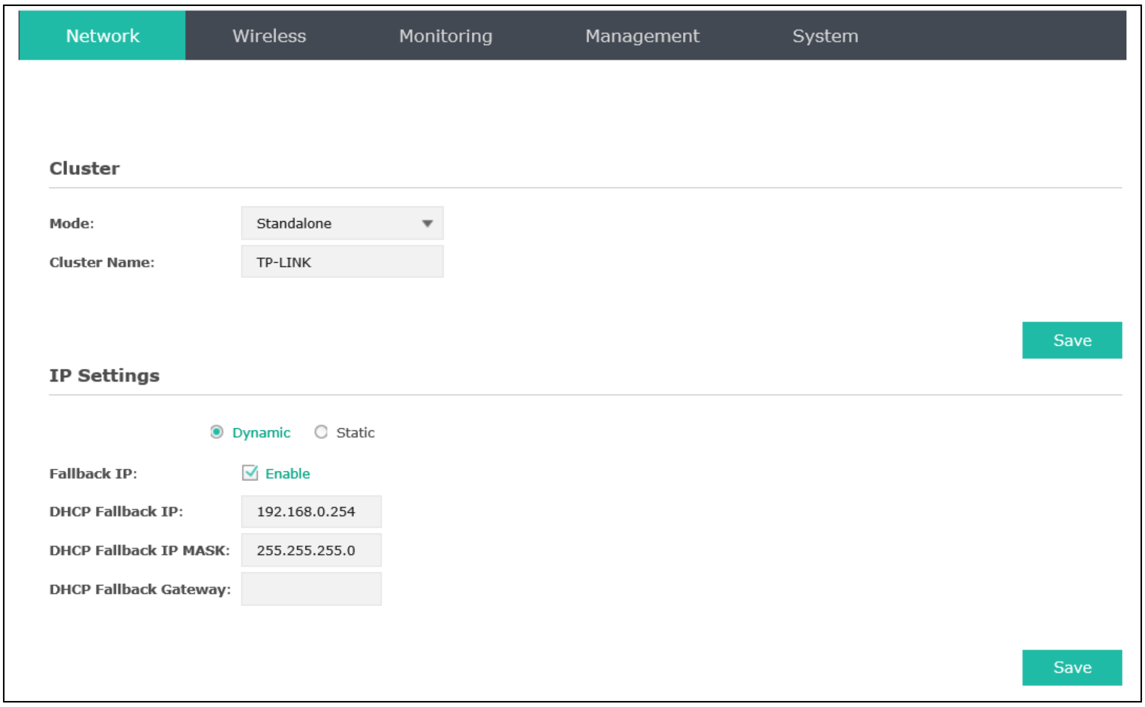
NOTE:

1. Please select the proper software version that matches your hardware to upgrade.
2. To avoid damage, please do not turn off the device while upgrading.
3. After upgrading, the device will reboot automatically.

Chapter 7 Standalone Mode

7.1 Network

On Network page you can configure the work mode and IP address of the standalone EAP.



Cluster

Mode: Standalone

Cluster Name: TP-LINK

IP Settings

● Dynamic ○ Static

Fallback IP: ☑ Enable

DHCP Fallback IP: 192.168.0.254

DHCP Fallback IP MASK: 255.255.255.0

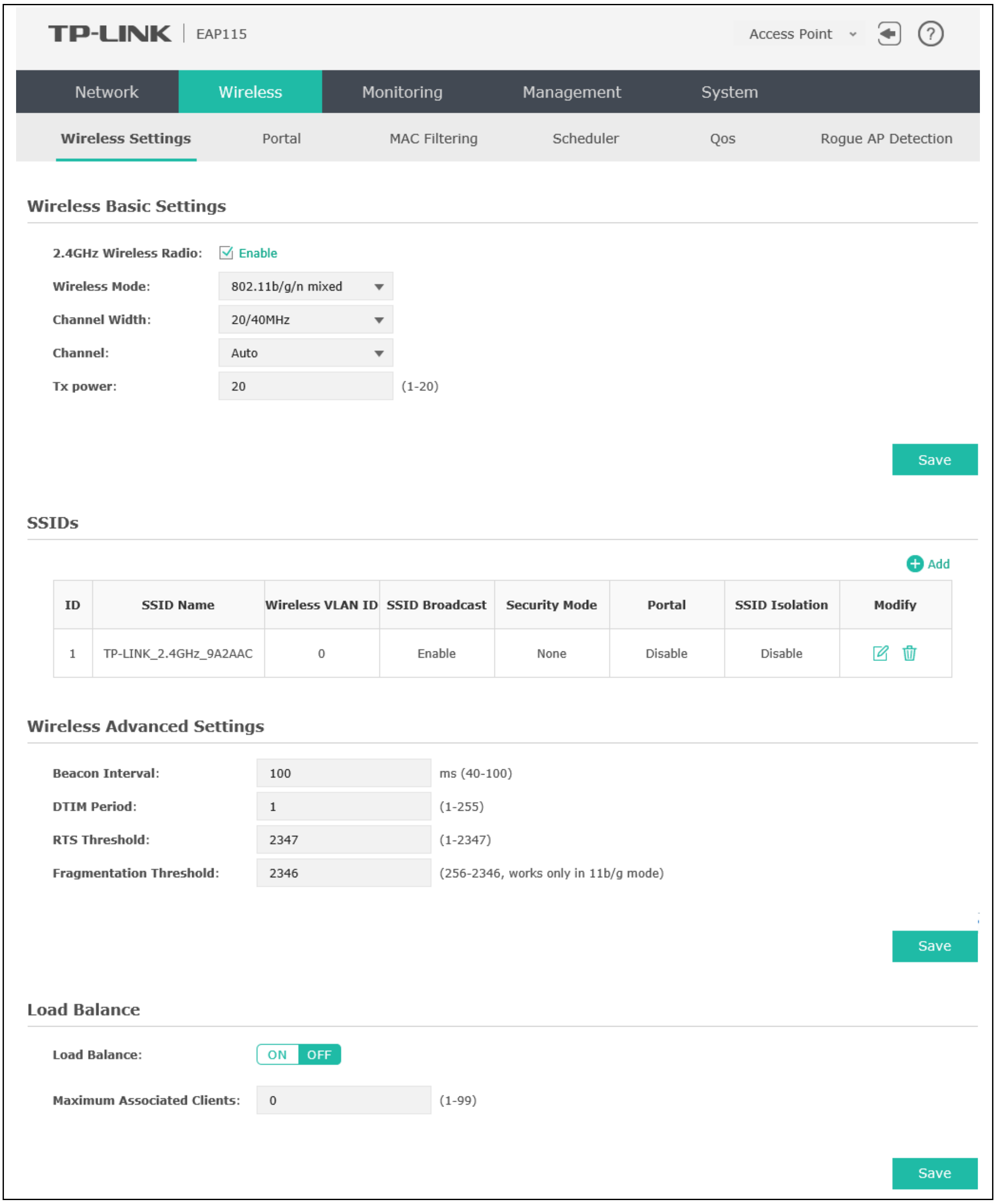
DHCP Fallback Gateway:

Figure 7-1 Network Page

Mode:	Choose the work mode of the EAP.
Cluster:	Enter the cluster name.
Dynamic/Static:	By default, the EAP device obtains an IP address from a DHCP server (typically a router). Select **Static** to configure IP address manually.
Fallback IP:	If the EAP fails to get a dynamic IP address from a DHCP server within ten seconds, the fallback IP will work as the IP address of the device. After that, however, the device will keep trying to obtain an IP address from the DHCP server until it succeeds.
DHCP Fallback IP/IP MASK:	Enter the fallback IP/IP mask.
DHCP Fallback Gateway:	Enter the fallback gateway.

7.2 Wireless

Wireless page, consisting of Wireless Settings, Portal, MAC Filtering, Scheduler, QoS and Rogue AP Detection, is shown below.



Wireless Basic Settings

2.4GHz Wireless Radio: ☑ Enable

Wireless Mode: 802.11b/g/n mixed

Channel Width: 20/40MHz

Channel: Auto

Tx power: 20 (1-20)

Save

SSIDs

Add

ID	SSID Name	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-LINK_2.4GHz_9A2AAC	0	Enable	None	Disable	Disable	

Wireless Advanced Settings

Beacon Interval: 100 ms (40-100)

DTIM Period: 1 (1-255)

RTS Threshold: 2347 (1-2347)

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

Save

Load Balance

Load Balance: ON OFF

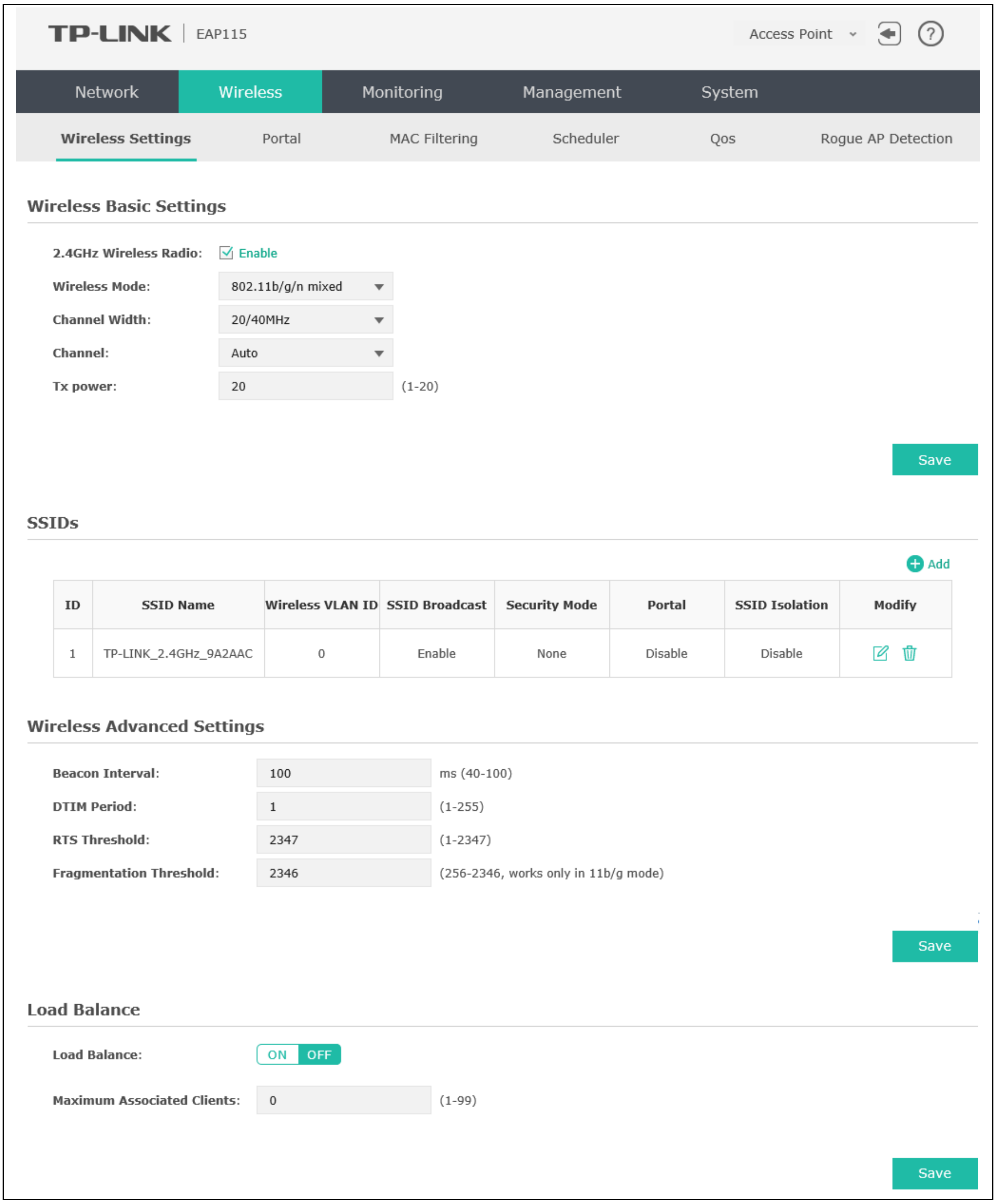
Maximum Associated Clients: 0 (1-99)

Save

Figure 7-2 Wireless Page

7.2.1 Wireless Settings

Following is the page of Wireless Settings.



Wireless Basic Settings

2.4GHz Wireless Radio: ☑ Enable

Wireless Mode: 802.11b/g/n mixed

Channel Width: 20/40MHz

Channel: Auto

Tx power: 20 (1-20)

Save

SSIDs

Add

ID	SSID Name	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-LINK_2.4GHz_9A2AAC	0	Enable	None	Disable	Disable	

Wireless Advanced Settings

Beacon Interval: 100 ms (40-100)

DTIM Period: 1 (1-255)

RTS Threshold: 2347 (1-2347)

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

Save

Load Balance

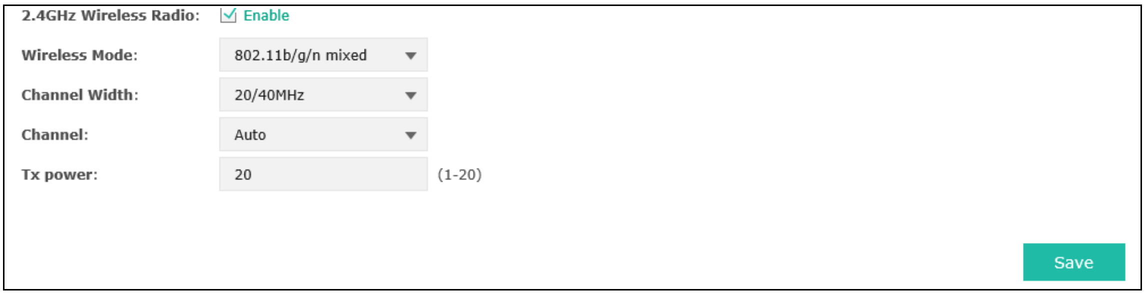
Load Balance: ON OFF

Maximum Associated Clients: 0 (1-99)

Save

Figure 7-3 Wireless Settings Page

7.2.1.1 Wireless Basic Settings



2.4GHz Wireless Radio: ☑ Enable

Wireless Mode: 802.11b/g/n mixed

Channel Width: 20/40MHz

Channel: Auto

Tx power: 20 (1-20)

Figure 7-4 Wireless Basic Settings

2.4GHz Wireless Radio:

Check the box to enable 2.4GHz Wireless Radio.

Wireless Mode:

Select the protocol standard for the wireless network.

Wireless network created by the EAP is able to operate in the 2.4GHz frequency The EAP supports 802.11b/g/n, 802.11b/g, and 802.11n standards. It is recommended to select 802.11b/g/n, in which way clients supporting 11b, 11g or 11n mode can access your wireless network.

Channel Width:

Select the channel width of this device. Options include 20MHz, 40MHz and 20/40MHz (this device automatically selects 20MHz or 40MHz, and 20MHz will be used if 40MHz is not available). According to IEEE 802.11n standard, using a channel width of 40MHz can increase wireless throughput. However, users may choose lower bandwidth due to the following reasons:

1. To increase the available number of channels within the limited total bandwidth.
2. To avoid interference from overlapping channels occupied by other devices in the environment.
3. Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances.

Channel:

Select the channel used by this device to improve wireless performance. 1/2412MHz means the Channel is 1 and the frequency is 2412MHz. The channel number varies in different regions. By default, channel is automatically selected.

Tx power:

Enter the transmit power value. By default, the value is 20. The maximum transmit power may vary among different countries or regions.

If the maximum transmit power is set to be larger than local regulation allows, the maximum Tx power regulated will be applied in actual situation.

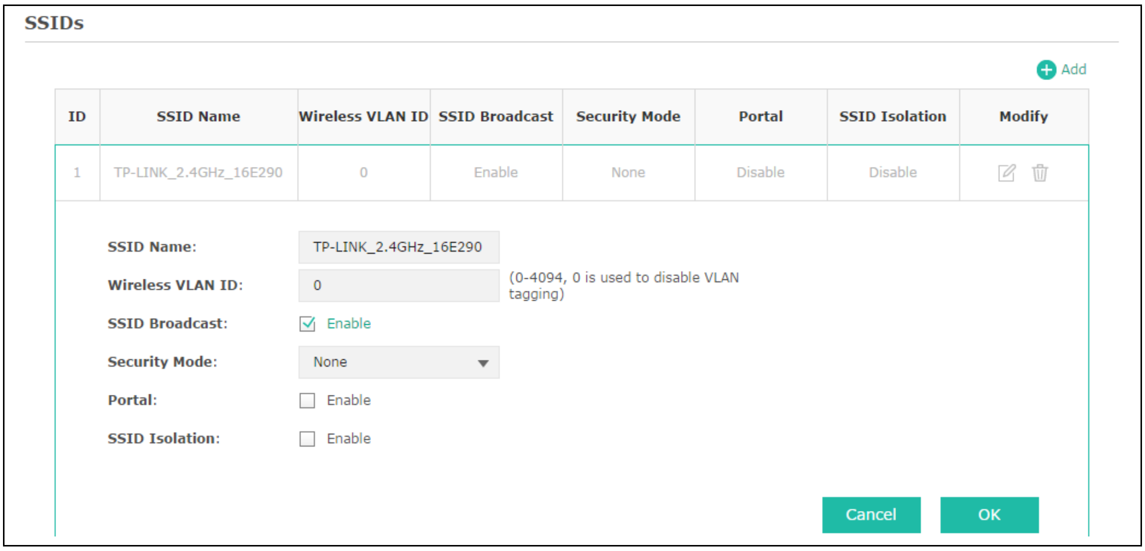
NOTE: In most cases, it is unnecessary to select maximum transmit power. Selecting larger transmit power than needed may cause interference to neighborhood. Also it consumes more power and will reduce longevity of the device. Select a certain transmit power is enough to achieve the best performance.

7.2.1.2 SSIDs

SSIDs can work together with switches supporting 802.1Q VLAN. The EAP can build up to eight virtual wireless networks per radio for users to access. At the same time, it adds different VLAN tags to the clients which connect to the corresponding wireless network. It supports maximum 8 VLANs per radio. The clients in different VLAN cannot directly communicate with each other.

Clients connected to the device via cable do not belong to any VLAN. Thus wired client can communicate with all the wireless clients despite the VLAN settings.

Click ✎ in the Modify column, the following content will be shown.



SSIDs

+ Add

ID	SSID Name	Wireless VLAN ID	SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify
1	TP-LINK_2.4GHz_16E290	0	Enable	None	Disable	Disable	✎ 🗑

SSID Name: TP-LINK_2.4GHz_16E290

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

SSID Broadcast: ☑ Enable

Security Mode: None ▼

Portal: □ Enable

SSID Isolation: □ Enable

Figure 7-5 SSIDs

+ Add Click to add up to 8 wireless networks per radio.

SSID Name: Enter up to 32 characters as the SSID name.

Wireless VLAN ID: Set a VLAN ID (ranges from 0 to 4094) for the wireless network. VLAN 0 means VLAN function is disabled. Wireless networks with the same VLAN ID are grouped to a VLAN.

SSID Broadcast: Enable this function, AP will broadcast its SSID to hosts in the surrounding environment, as thus hosts can find the wireless network identified by this SSID. If SSID Broadcast is not enabled, hosts must enter the AP's SSID manually to connect to this AP.

Security Mode: Select the security mode of the wireless network. For the security of wireless network, you are suggested to encrypt your wireless network. This device provides three security modes: **WPA-Enterprise**, **WPA-PSK** (WPA Pre-Shared Key) and **WEP** (Wired Equivalent Privacy). WPA-PSK is recommended. Settings vary in different security modes as the details are in the following introduction. Select **None** and the hosts can access the wireless network without password.

Portal: Portal provides authentication service for the clients who want to access the wireless local area network. For more information, refer to 7.2.2 Portal. After Portal is enabled, the configurations in 7.2.2 Portal will be applied.

SSID Isolation: After enabling SSID Isolation, the devices connected in the same SSID cannot communicate with each other.

Modify: Click ✎ to open the page to edit the parameters of SSID.

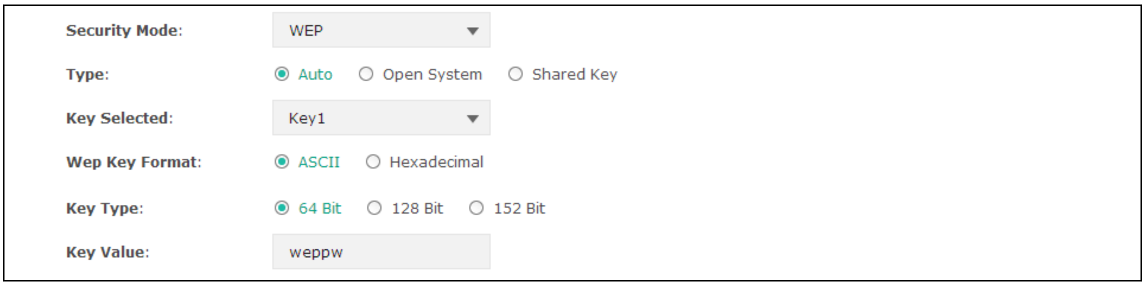
Click 🗑 to delete the SSID.

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

- ## WEP

WEP (Wired Equivalent Privacy), based on the IEEE 802.11 standard, is less safe than WPA-Enterprise or WPA-PSK.

> ***NOTE:***
>
> WEP is not supported in 802.11n mode. If WEP is applied in 802.11n mode, the clients may not be able to access the wireless network. If WEP is applied in 11b/g/n mode (in the 2.4GHz frequency band), the device may work at a low transmission rate.



Security Mode:	WEP ▼
Type:	● Auto ○ Open System ○ Shared Key
Key Selected:	Key1 ▼
Wep Key Format:	● ASCII ○ Hexadecimal
Key Type:	● 64 Bit ○ 128 Bit ○ 152 Bit
Key Value:	weppw

Figure 7-6 Security Mode_WEP

Type: Select the authentication type for WEP.

- **Auto**: The default setting is Auto, which can select Open System or Shared Key automatically based on the wireless station's capability and request.
- **Open System**: After you select 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**: After you select Shared Key, clients has to input password to pass the authentication, or it cannot associate with the wireless network or transmit data.

Key Selected: You can configure four keys in advance and select one as the present valid key.

Wep Key Format: Select the wep key format ASCII or Hexadecimal.

- **ASCII**: ASCII format stands for any combination of keyboard characters in the specified length.

- **Hexadecimal**: Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

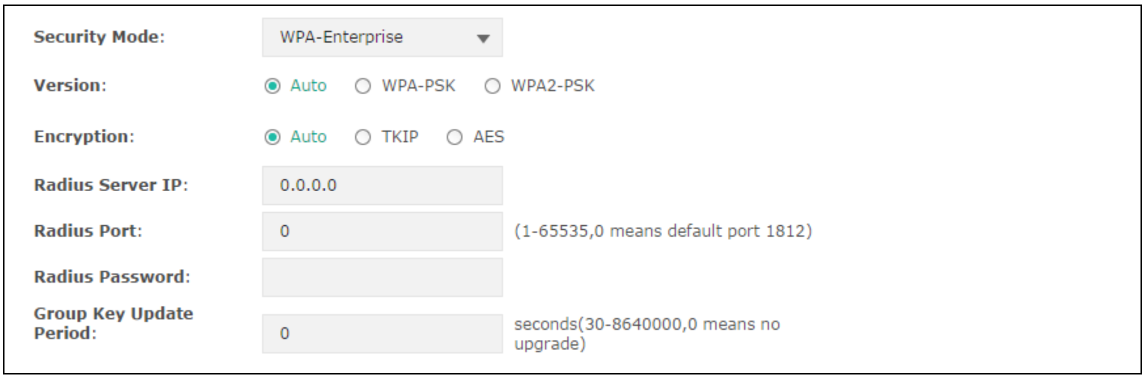
Key Type: Select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption.

- **64-bit**: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F without null key) or 5 ASCII characters.
- **128-bit**: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F without null key) or 13 ASCII characters.
- **152-bit**: You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F without null key) or 16 ASCII characters.

Key Value: Enter the key value.

WPA-Enterprise

Based on RADIUS server, WPA-Enterprise can generate different passwords for different users and it is much safer than WPA-PSK. However, it costs much to maintain and is more suitable for enterprise users. At present, WPA-Enterprise has two versions: WPA-PSK and WPA2-PSK.



Security Mode: WPA-Enterprise

Version: ● Auto ○ WPA-PSK ○ WPA2-PSK

Encryption: ● Auto ○ TKIP ○ AES

Radius Server IP: 0.0.0.0

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

Radius Password:

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

Figure 7-7 Security Mode_WPA-Enterprise

Version: Select one of the following versions:

- **Auto**: Select WPA-PSK or WPA2-PSK automatically based on the wireless station's capability and request.
- **WPA-PSK**: Pre-shared key of WPA.
- **WPA2-PSK**: Pre-shared key of WPA2.

Encryption: Select the encryption type, including **Auto**, **TKIP**, and **AES**. The default setting is Auto, which can select TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) automatically based on the wireless station's capability and request. AES is more secure than TKIP and TKIP is not supported in 802.11n mode. It is recommended to select AES as the encryption type.

RADIUS Server IP/Port: Enter the IP address/port of the RADIUS server.

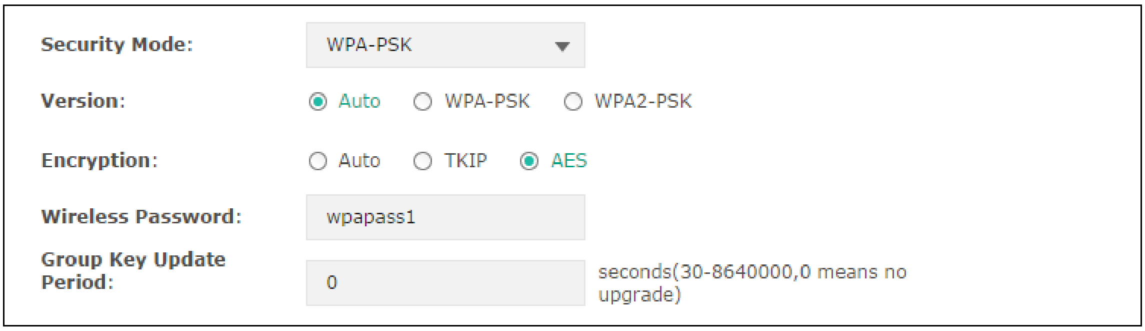
RADIUS Password:	Enter the shared secret of RADIUS server to access the RADIUS server.
Group Key Update period:	Specify the group key update period in seconds. The value can be either 0 or at least 30. 0 means no update.

NOTE:

Encryption type TKIP is not supported in 802.11n mode. If TKIP is applied in 802.11n mode, the clients may not be able to access the wireless network of the EAP. If TKIP is applied in 11b/g/n mode (in the 2.4GHz frequency band), the device may work at a low transmission rate.

WPA-PSK

Based on pre-shared key, security mode WPA-PSK is characterized by high security and simple configuration, which suits for common households and small business. WPA-PSK has two versions: WPA-PSK and WPA2-PSK.



Security Mode: WPA-PSK

Version: ● Auto ○ WPA-PSK ○ WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

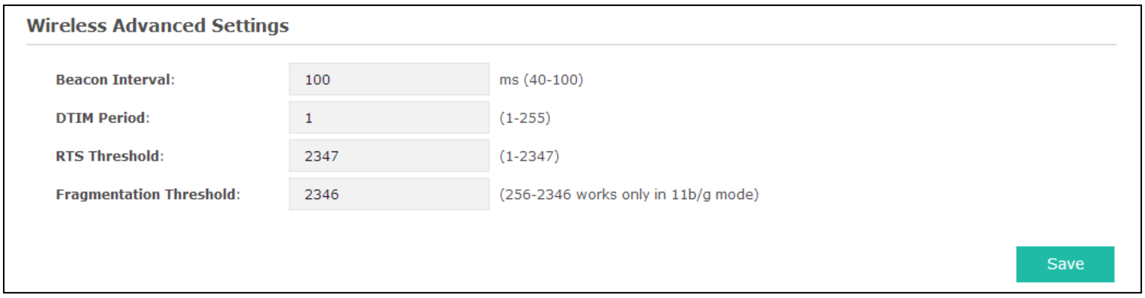
Wireless Password: wpapass1

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

Figure 7-8 Security Mode_WPA-PSK

Version:	• **Auto**: Select WPA or WPA2 automatically based on the wireless station's capability and request. • **WPA**: Pre-shared key of WPA. • **WPA2**: Pre-shared key of WPA2.
Encryption:	Select the encryption type, including **Auto**, **TKIP**, and **AES**. The default setting is Auto, which can select TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) automatically based on the wireless station's capability and request. AES is more secure than TKIP and TKIP is not supported in 802.11n mode. It is recommended to select AES as the encryption type.
Wireless Password:	Configure the WPA-PSK/WPA2-PSK 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 the group key update period in seconds. The value can be either 0 or at least 30. 0 means no update.

7.2.1.3 Wireless Advanced Settings


Wireless Advanced Settings

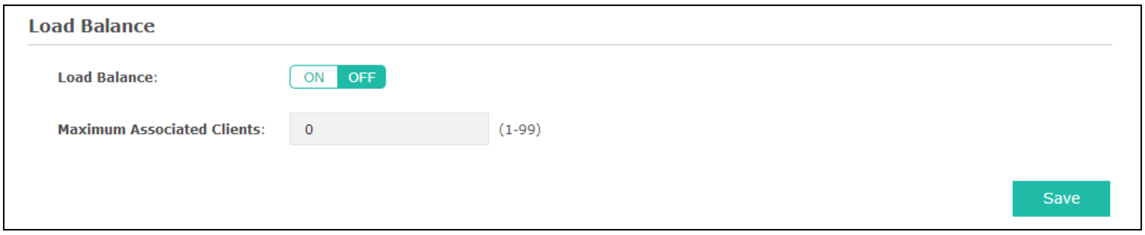
Beacon Interval:	100	ms (40-100)
DTIM Period:	1	(1-255)
RTS Threshold:	2347	(1-2347)
Fragmentation Threshold:	2346	(256-2346 works only in 11b/g mode)

Figure 7-9 Wireless Advanced Settings

Beacon Interval:	Beacons are transmitted periodically by the 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 from 40 to 100. The default value is 100 milliseconds.
DTIM Period:	This value indicates the number of beacon intervals between successive Delivery Traffic Indication Messages (DTIMs) and this number is included in each Beacon frame. A DTIM is contained in Beacon frames to indicate whether the access point has buffered broadcast and/or multicast data for the client devices. Following a Beacon frame containing a DTIM, the access point will release the buffered broadcast and/or multicast data, if any exists. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating the DTIM Period is the same as Beacon Interval. An excessive DTIM period may reduce the performance of multicast applications. It is recommended to keep it by default.
RTS Threshold:	When the RTS threshold is activated, all the stations and APs follow the Request to Send (RTS) protocol. When the station is to send packets, it will send a RTS to AP to inform the AP that it will send data. After receiving the RTS, the AP notices other stations in the same wireless network to delay their transmitting of data. At the same time, the AP inform the requesting station to send data. The value range is from 1 to 2347 bytes. The default value is 2347, which means that RTS is disabled.
Fragmentation Threshold:	Specify the fragmentation threshold for packets. If the size of the packet is larger than the fragmentation threshold, the packet will be fragmented into several packets. Too low fragmentation threshold may result in poor wireless performance caused by the excessive packets. The recommended and default value is 2346 bytes.

7.2.1.4 Load Balance

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


Load Balance

Load Balance: ON OFF

Maximum Associated Clients: 0 (1-99)

Figure 7-10 Load Balance

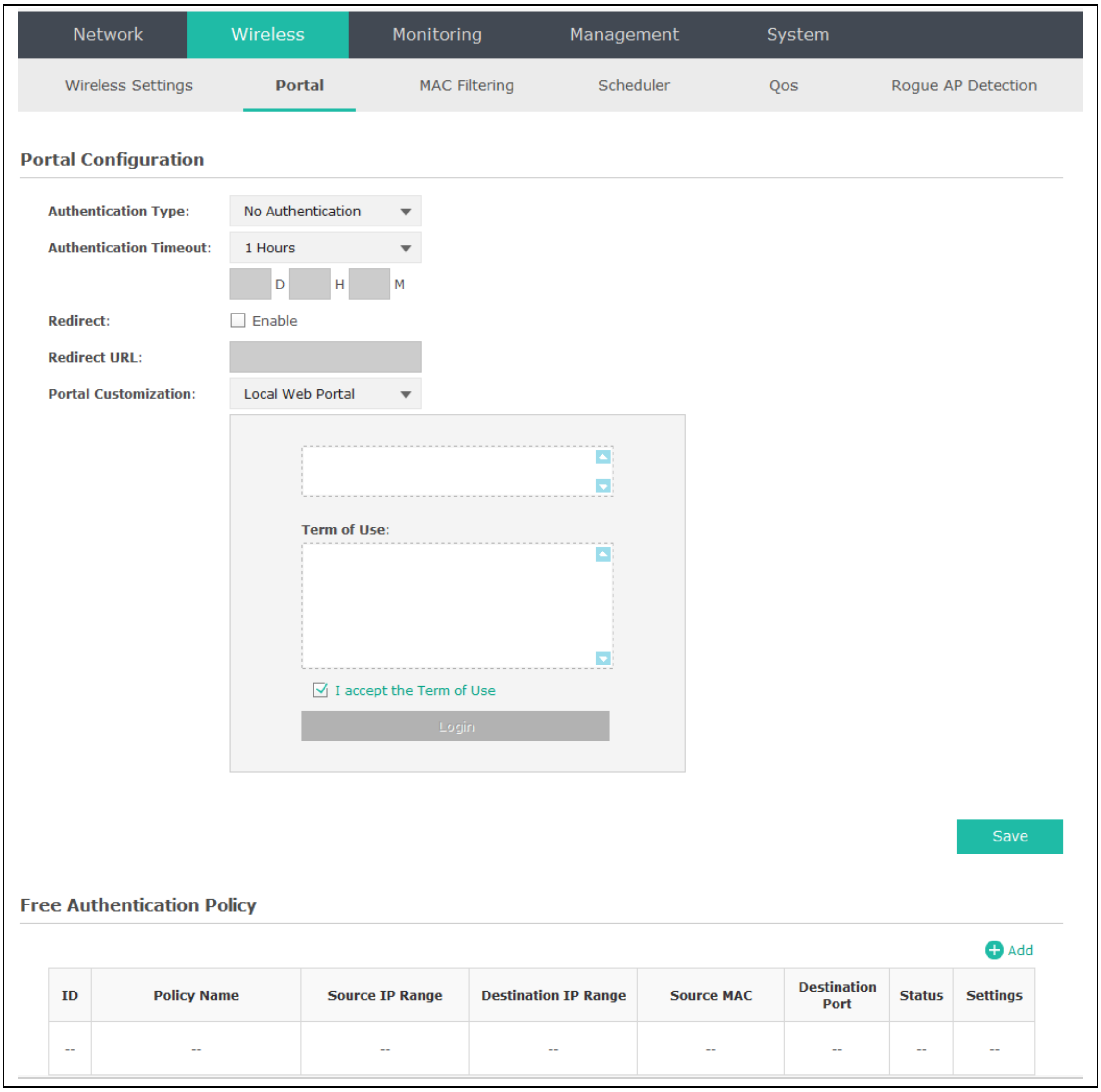
Load Balance:	Disable by default. Click **ON** to enable the function. After enabling it, you can set a number for maximum associated clients to control the wireless access.
Maximum Associated Clients:	Enter the number of clients to be allowed for connection to the EAP. The number ranges from 1 to 99.

7.2.2 Portal

Portal authentication enhances the network security by providing authentication service to the clients who want to access the wireless local network. Portal is also called web authentication. The users have to log in a web page to establish verification.

Network resources can be classified into different types for different users. Part of them can be accessed for free by the clients; while some specific resources can only be accessed by authorized users. What's more, you can customize the authentication login page and specify a URL which the newly authenticated client will be redirected to. Please refer to Portal Configuration or Free Authentication Policy according to your need.

Following is the page of Portal.



Portal Configuration

Authentication Type: No Authentication

Authentication Timeout: 1 Hours

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal

Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Figure 7-11 Portal Page

NOTE:

To apply Portal in a wireless network, please go to **Wireless→Wireless Settings→SSIDs** to enable Portal of a selected SSID.

7.2.2.1 Portal Configuration

Three authentication types are available: No Authentication, Local Password and External RADIUS Server.

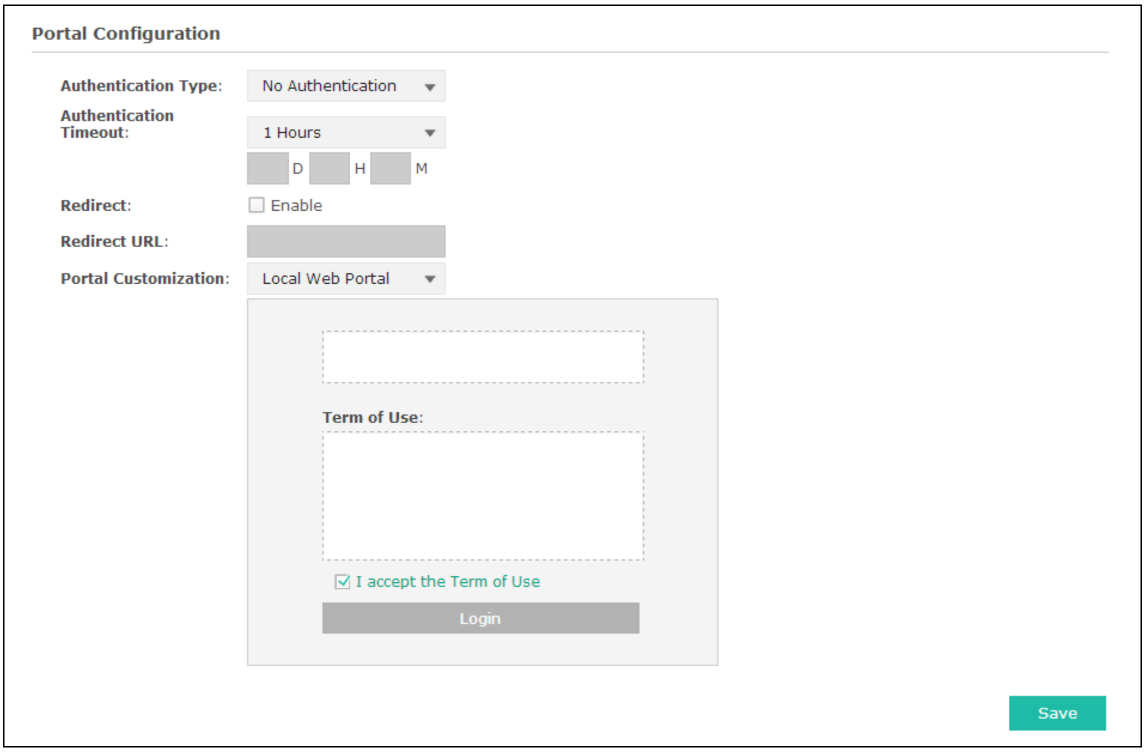
1. No Authentication： Users are required to finish only two steps: agree with the user protocol and click the **Login** button.

2. Local Password: Users are required to enter the preset user name and password, which are saved in the EAP.

3. External RADIUS Server: Users are required to enter the preset user name and password, which are saved in the database of the RADIUS server. The RADIUS server acts as the authentication server, which allows you to set different user name and password for different users.

Refer to the following content to configure Portal based on actual network situations.

No Authentication



Portal Configuration

Authentication Type: No Authentication

Authentication Timeout: 1 Hours

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal

Term of Use:

☑ I accept the Term of Use

Login

Save

Figure 7-12 Portal Configuration_No Authentication

Authentication Type: Select **No Authentication**.

Authentication Timeout: After successful verification, an authentication session is established. Authentication Timeout decides the active time of the session. Within the active time, the device keeps the authentication session open with the associated client. To reopen the session, the client needs to log in the web authentication page and enter the user name and password again once authentication timeout is reached.

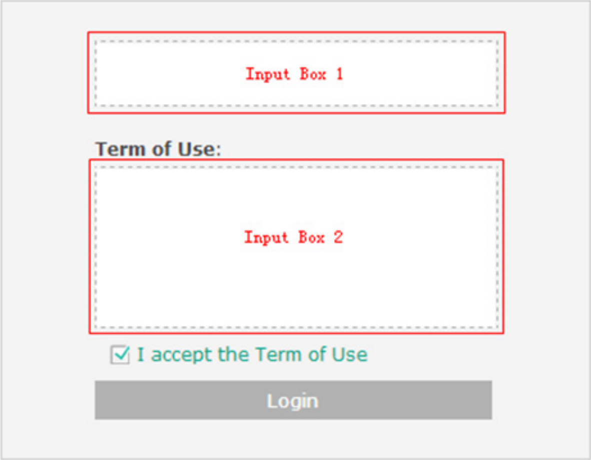
By default, authentication timeout is one hour. Select **Custom** from the drop-down list to customize the parameter.

Redirect: Disable by default. Redirect specifies that the portal should redirect the newly authenticated clients to the configured URL.

Redirect URL: Enter the URL that a newly authenticated client will be directed to.

Portal Customization: Select Local Web Portal, the authentication login page will be provided by the built-in portal server.

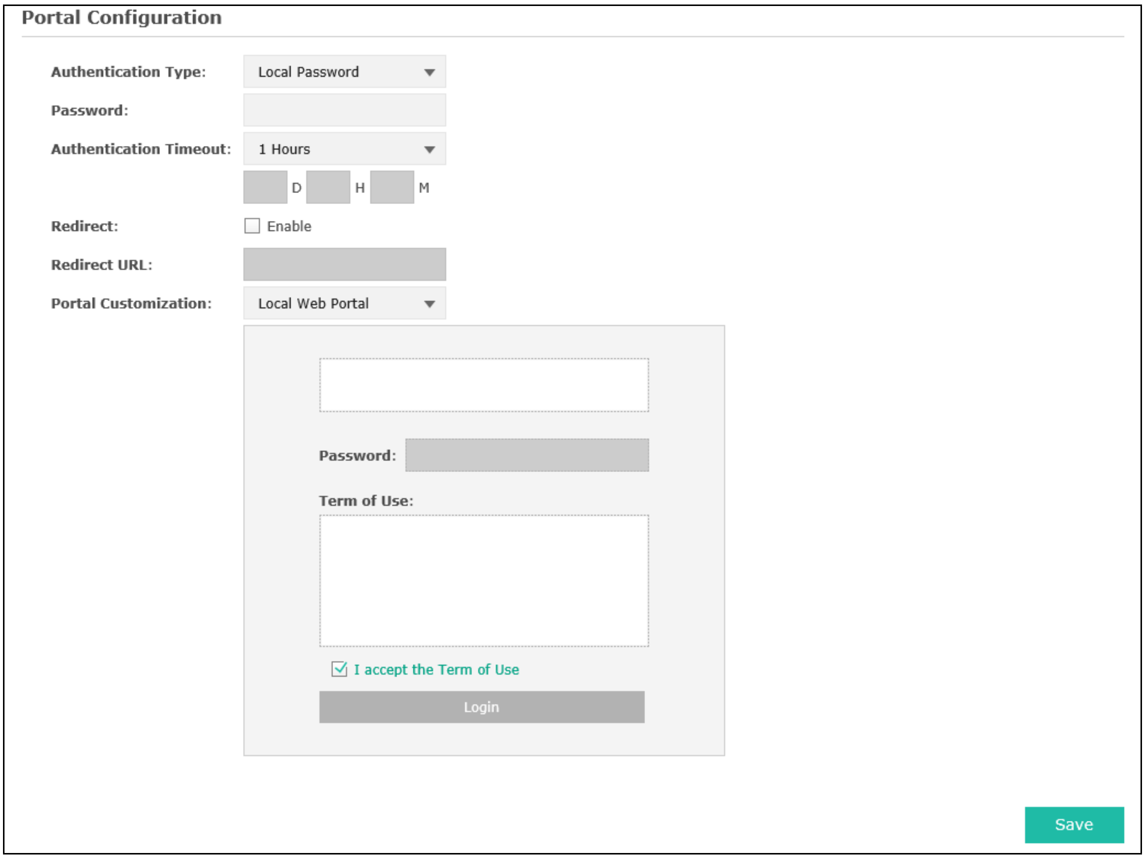
The page configured below will be presented to users as the login page. Words can be filled in Input Box 1 and Input Box 2.



Enter up to 31 characters as the title of the authentication login page in Input Box 1, like “Guest Portal of TP-LINK”.

Enter the terms presented to users in Input Box 2. The terms can be 1 to 1023 characters long.

Local Password



Portal Configuration

Authentication Type: Local Password

Password:

Authentication Timeout: 1 Hours

D H M

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal

Password:

Term of Use:

☑ I accept the Term of Use

Figure 7-13 Portal Configuration_Local Password

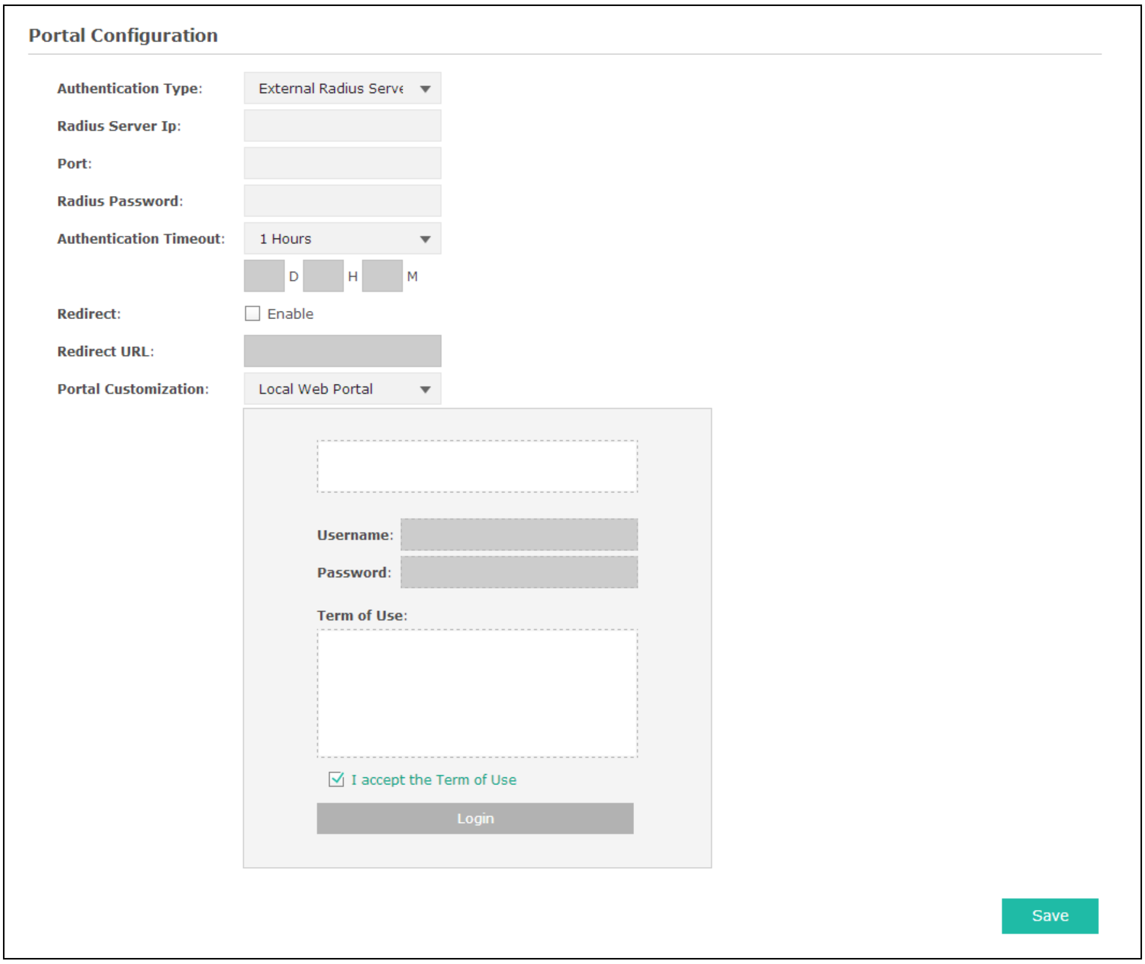
Authentication Type:	Select **Local Password**.
Password:	Enter the password for local authentication.

Please refer to No Authentication to configure **Authentication Timeout**, **Redirect**, **Redirect URL**, and **Portal Customization**.

External RADIUS Server

External RADIUS Server provides 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, as Figure 6-25 shown. The authentication login page of External Web Portal is provided by external portal server, as Figure 6-26 shown.

1. Local Web Portal



Portal Configuration

Authentication Type: External Radius Serve

Radius Server Ip:

Port:

Radius Password:

Authentication Timeout: 1 Hours

Redirect: □ Enable

Redirect URL:

Portal Customization: Local Web Portal

Username:

Password:

Term of Use:

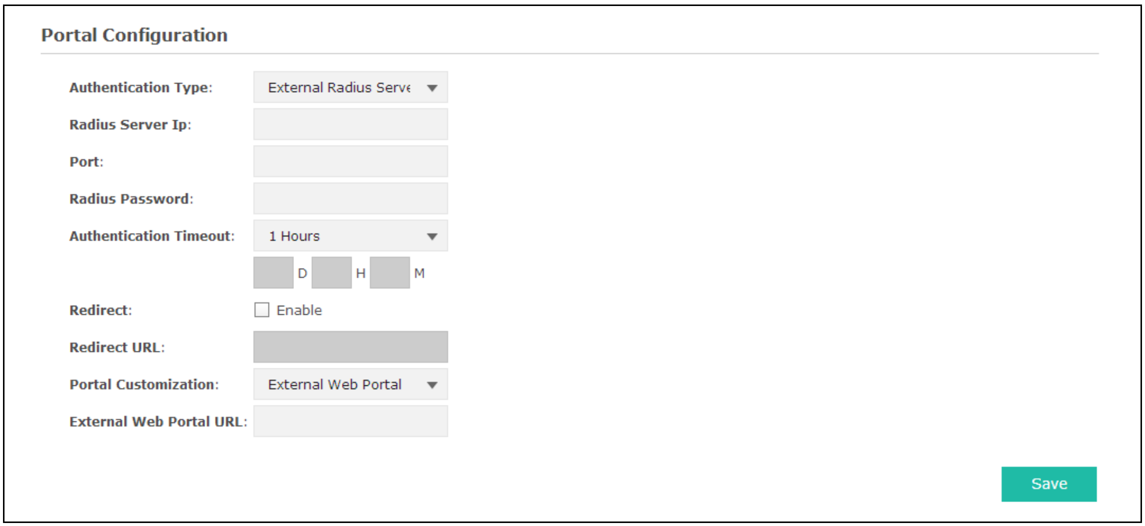
☑ I accept the Term of Use

Figure 7-14 Portal Configuration_External RADIUS Server_Local Web Portal

Authentication Type:	Select **External RADIUS Server**.
RADIUS Server IP:	Enter the IP address of the RADIUS server.
Port:	Enter the port for authentication service.
RADIUS Password:	Enter the shared secret of RADIUS server to log in to the RADIUS server.

Please refer to No Authentication to configure **Authentication Timeout**, **Redirect**, **Redirect URL**, and **Portal Customization**.

2. External Web Portal



Portal Configuration

Authentication Type:	External Radius Serve ▼
Radius Server Ip:	
Port:	
Radius Password:	
Authentication Timeout:	1 Hours ▼
	D H M
Redirect:	□ Enable
Redirect URL:	
Portal Customization:	External Web Portal ▼
External Web Portal URL:	

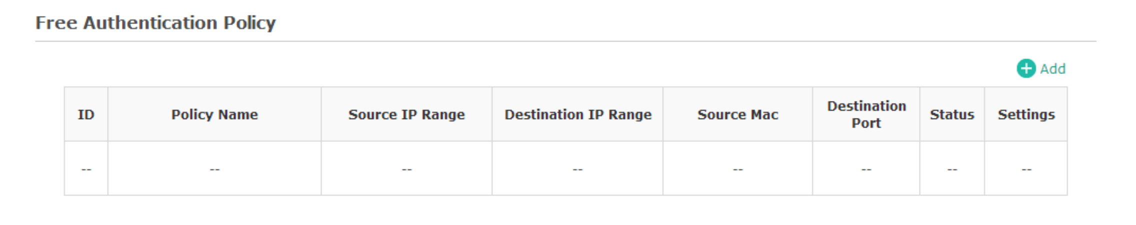
Figure 7-15 Portal Configuration_External RADIUS Server_External Web Portal

Authentication Type:	Select **External RADIUS Server**.
RADIUS Server IP:	Enter the IP address of the RADIUS server.
Port:	Enter the port for authentication service.
RADIUS Password:	Enter the shared secret of RADIUS server to log in to the RADIUS server.
Portal Customization:	Select **External Web Portal**.
External Web Portal URL:	Enter the authentication login page's URL, which is provided by the remote portal server.

Please refer to No Authentication to configure **Authentication Timeout**, **Redirect** and **Redirect URL**.

7.2.2.2 Free Authentication Policy

Free Authentication Policy allows clients to access network resources for free. On the lower part of the Portal page you can configure and view free authentication policies.

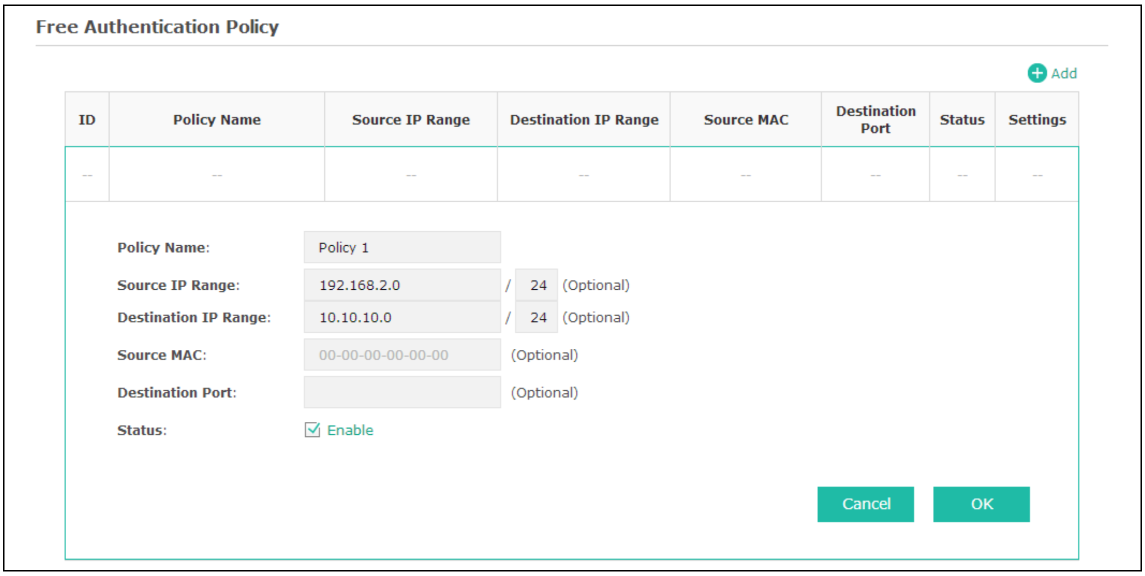


Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source Mac	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Figure 7-16 Free Authentication Policy

Click ⊕ Add to add a new authentication policy and configure its parameters.



Free Authentication Policy

⊕ Add

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Settings
--	--	--	--	--	--	--	--

Policy Name: Policy 1

Source IP Range: 192.168.2.0 / 24 (Optional)

Destination IP Range: 10.10.10.0 / 24 (Optional)

Source MAC: 00-00-00-00-00-00 (Optional)

Destination Port: (Optional)

Status: ☑ Enable

Figure 7-17 Configure Free Authentication Policy

Policy Name: Enter a policy name.

Source IP Range: Enter the source IP address and subnet mask of the clients who can enjoy the free authentication policy. Leaving the field empty means all IP addresses can access the specific resources.

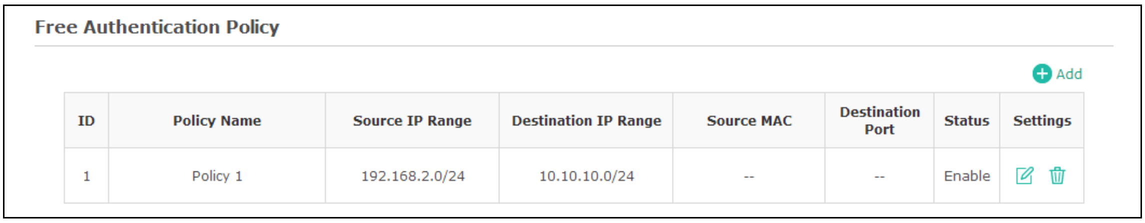
Destination IP Range: Enter the destination IP address and subnet mask for free authentication policy. Leaving the field empty means all IP addresses can be visited. When **External Radius Server** is configured and **External Web Portal** is selected, please set the IP address and subnet mask of your external web server as the **Destination IP Range**.

Source MAC: Enter the source MAC address of the clients who can enjoy the free authentication policy. Leaving the field empty means all MAC addresses can access the specific resources.

Destination Port: Enter the destination port for free authentication policy. Leaving the field empty means all ports can be accessed.

Status: Check the box to enable the policy.

Click the button **OK** in Figure 6-28 and the policy is successfully added as Figure 6-29 shows.



Free Authentication Policy

ID	Policy Name	Source IP Range	Destination IP Range	Source MAC	Destination Port	Status	Settings
1	Policy 1	192.168.2.0/24	10.10.10.0/24	--	--	Enable	

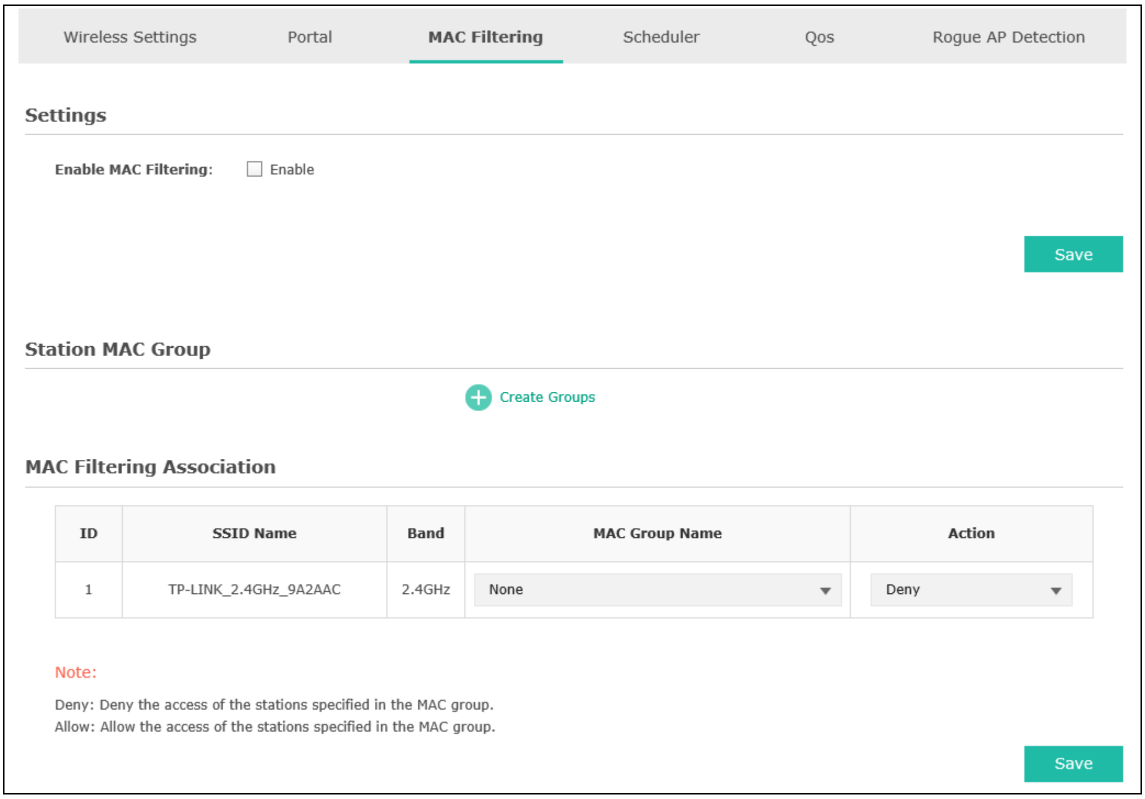
Figure 7-18 Add Free Authentication Policy

Here is the explanation of Figure 6-29: The policy name is Policy 1. Clients with IP address range 192.168.2.0/24 are able to visit IP range 10.10.10.0/24. Policy 1 is enabled.

Click to edit the policy. Click to delete the policy.

7.2.3 MAC Filtering

MAC Filtering uses MAC addresses to determine whether one host can access the wireless network or not. Thereby it can effectively control the user access in the wireless network.



Settings

Enable MAC Filtering: □ Enable

Station MAC Group

MAC Filtering Association

ID	SSID Name	Band	MAC Group Name	Action
1	TP-LINK_2.4GHz_9A2AAC	2.4GHz	None	Deny

Note:

Deny: Deny the access of the stations specified in the MAC group.
Allow: Allow the access of the stations specified in the MAC group.

Figure 7-19 MAC Filtering Page

- ## Settings

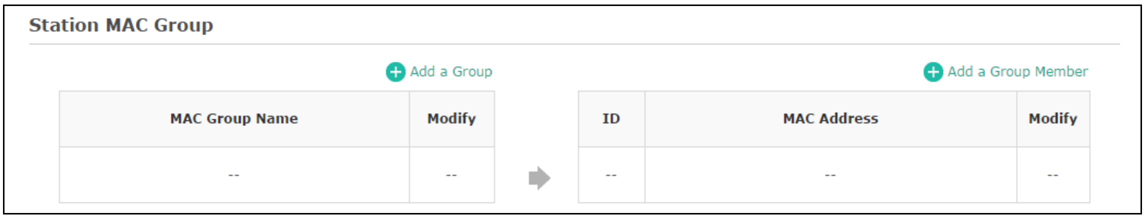
Enable MAC Filtering: Check the box to enable MAC Filtering.

- ## Station MAC Group

Follow the steps below to add MAC groups.

Step 1:

Click ⊕ Create Groups, two tables will be shown.



Station MAC Group

⊕ Add a Group

MAC Group Name	Modify
--	--

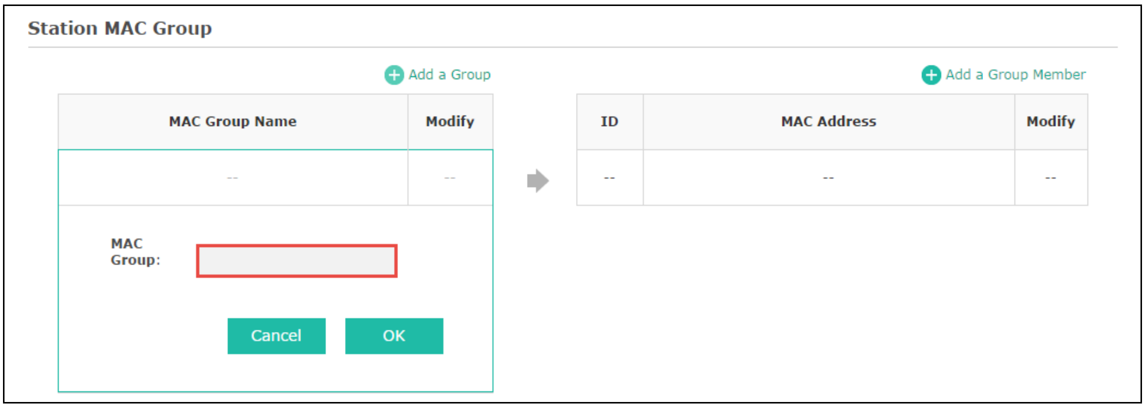
⊕ Add a Group Member

ID	MAC Address	Modify
--	--	--

Figure 7-20 Station MAC Group

Step 2:

Click ⊕ Add a Group and fill in a name for the MAC group.



Station MAC Group

⊕ Add a Group

MAC Group Name	Modify
--	--

MAC Group:

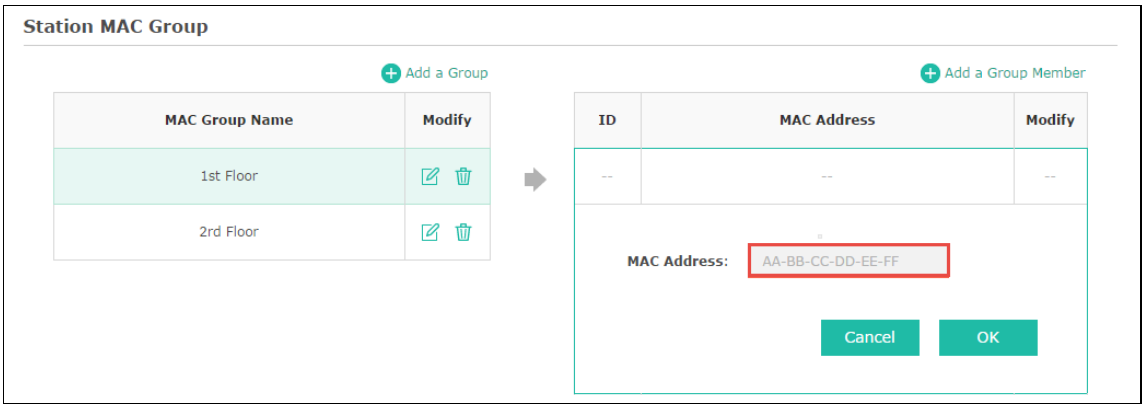
⊕ Add a Group Member

ID	MAC Address	Modify
--	--	--

Figure 7-21 Add a Group

Step 3:

Click ⊕ Add a Group Member and input the MAC address you want to organize into this group.



Station MAC Group

⊕ Add a Group

MAC Group Name	Modify
1st Floor	✎ 🗑
2rd Floor	✎ 🗑

⊕ Add a Group Member

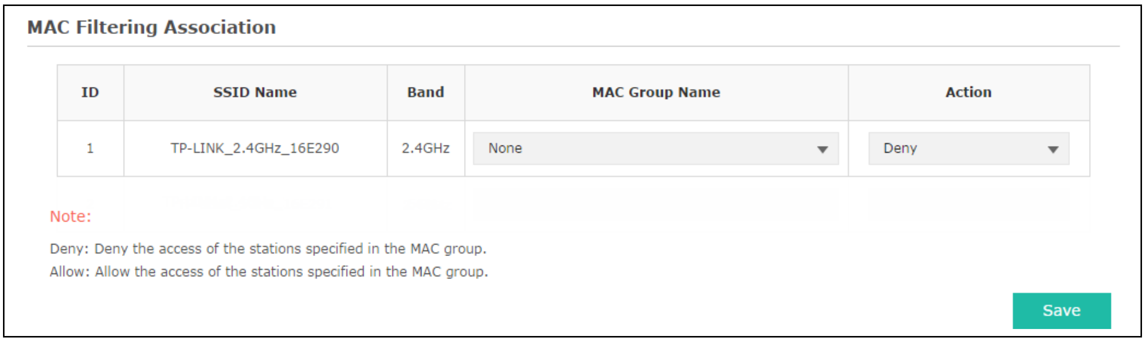
ID	MAC Address	Modify
--	--	--

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

Figure 7-22 Add a Group Member

Click ✎ in Modify column to edit the MAC group name or MAC address. Click 🗑 to delete the MAC group or group member.

- ## MAC Filtering Association



MAC Filtering Association

ID	SSID Name	Band	MAC Group Name	Action
1	TP-LINK_2.4GHz_16E290	2.4GHz	None ▾	Deny ▾

Note:

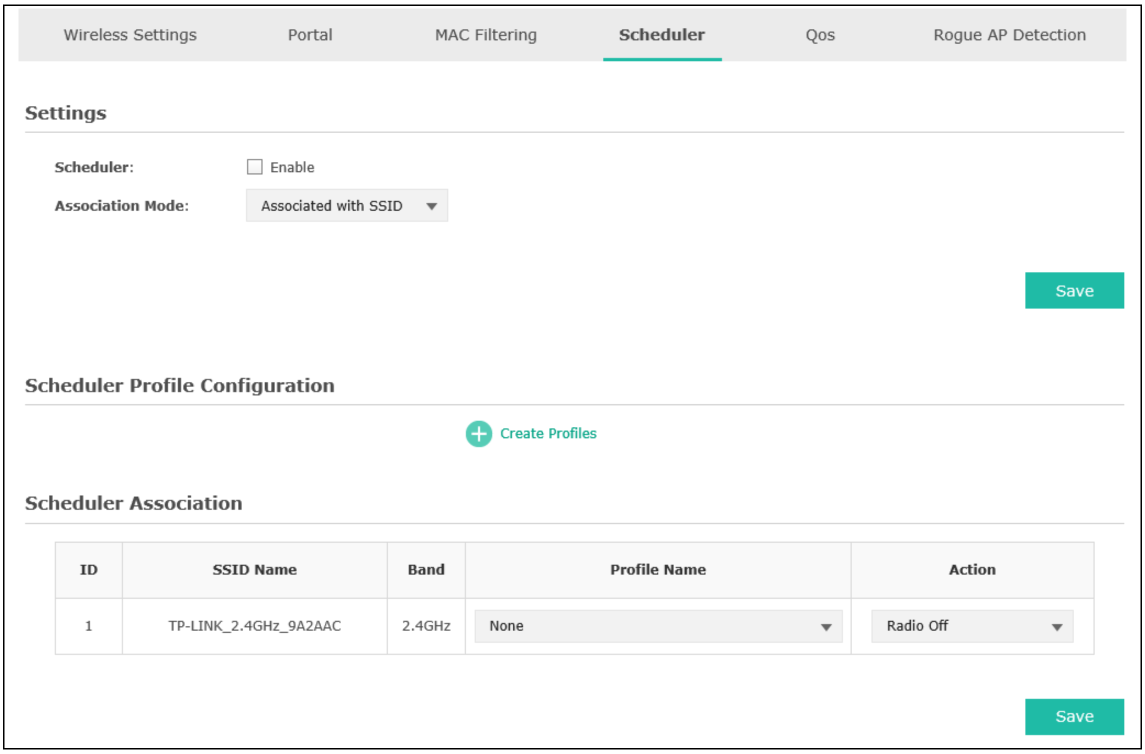
Deny: Deny the access of the stations specified in the MAC group.
Allow: Allow the access of the stations specified in the MAC group.

Figure 7-23 MAC Filtering Association

SSID Name:	Displays the SSID of the wireless network.
Band:	Displays the frequency band the wireless network operates at.
MAC Group Name:	Select a MAC group from the drop-down list to allow or deny its members to access the wireless network.
Action:	• **Allow**: Allow the access of the stations specified in the MAC group. • **Deny**: Deny the access of the stations specified in the MAC group.

7.2.4 Scheduler

Scheduler allows you to configure rules with specific time interval for radios to operate, which automates the enabling or disabling of the radio.



Wireless Settings | Portal | MAC Filtering | **Scheduler** | Qos | Rogue AP Detection

Settings

Scheduler: □ Enable

Association Mode: Associated with SSID ▼

Save

Scheduler Profile Configuration

⊕ Create Profiles

Scheduler Association

ID	SSID Name	Band	Profile Name	Action
1	TP-LINK_2.4GHz_9A2AAC	2.4GHz	None ▼	Radio Off ▼

Save

Figure 7-24 Scheduler Page

- ## Settings

Scheduler: Check the box to enable Scheduler.

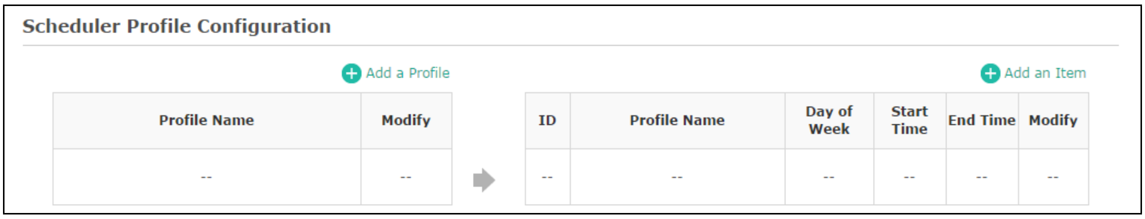
Association Mode: Select **Associated with SSID/AP**, you can perform configurations on the SSIDs/AP. The display of Scheduler Association is based on your option here.

- ## Scheduler Profile Configuration

Follow the steps below to add rules.

Step 1:

Click ⊕ Create Profiles, two tables will be shown.



Scheduler Profile Configuration

⊕ Add a Profile

Profile Name	Modify
--	--

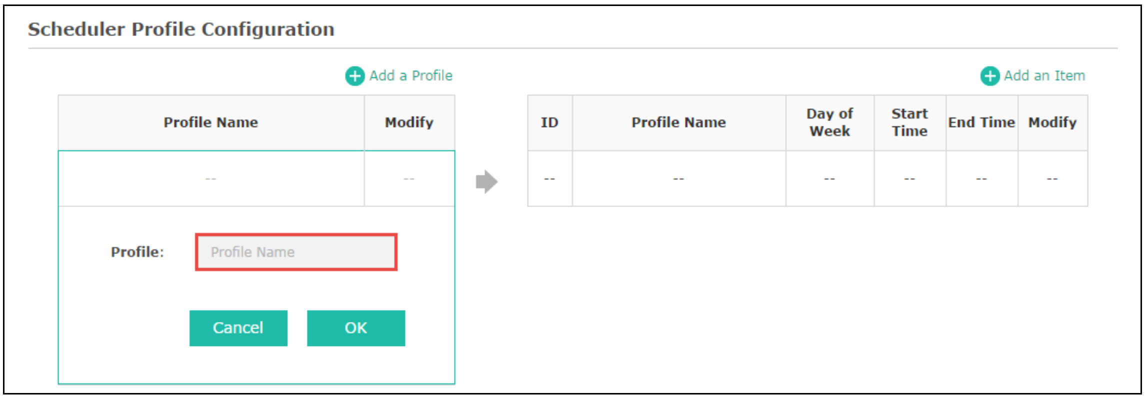
⊕ Add an Item

ID	Profile Name	Day of Week	Start Time	End Time	Modify
--	--	--	--	--	--

Figure 7-25 Scheduler Profile Configuration

Step 2:

Click ⊕ Add a Profile and input a profile name for the rule.



Scheduler Profile Configuration

Profile Name	Modify
--	--

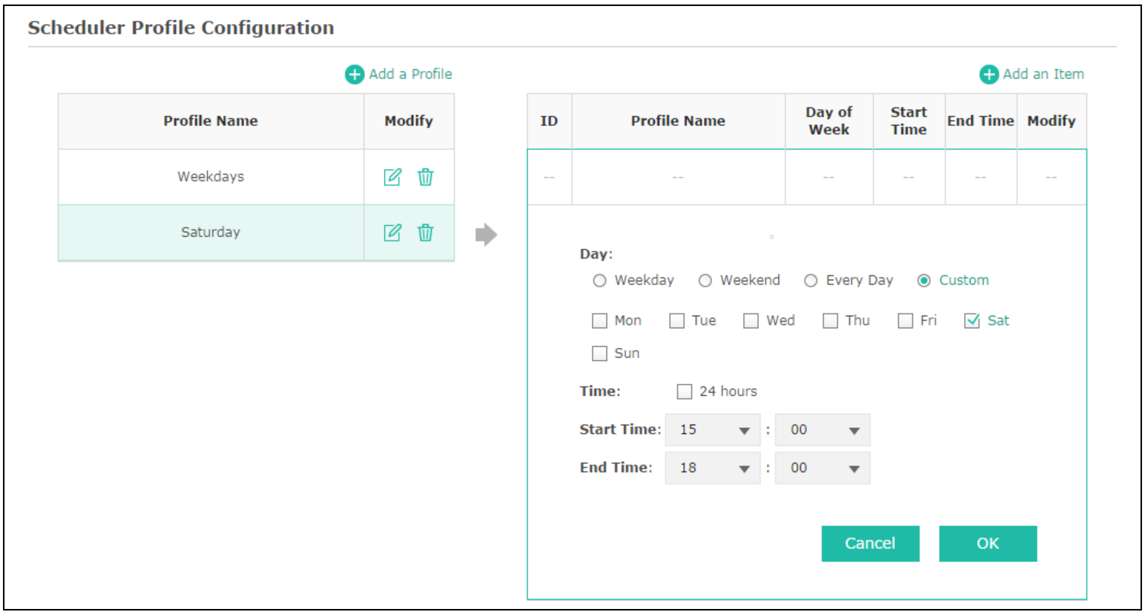
Profile: Profile Name

ID	Profile Name	Day of Week	Start Time	End Time	Modify
--	--	--	--	--	--

Figure 7-26 Add a Profile

Step 3:

Click ⊕ Add a Item and configure the recurring schedule for the rule.



Scheduler Profile Configuration

Profile Name	Modify
Weekdays	✎ 🗑
Saturday	✎ 🗑

ID	Profile Name	Day of Week	Start Time	End Time	Modify
--	--	--	--	--	--

Day: ○ Weekday ○ Weekend ○ Every Day ● Custom

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

Time: □ 24 hours

Start Time: 15 : 00

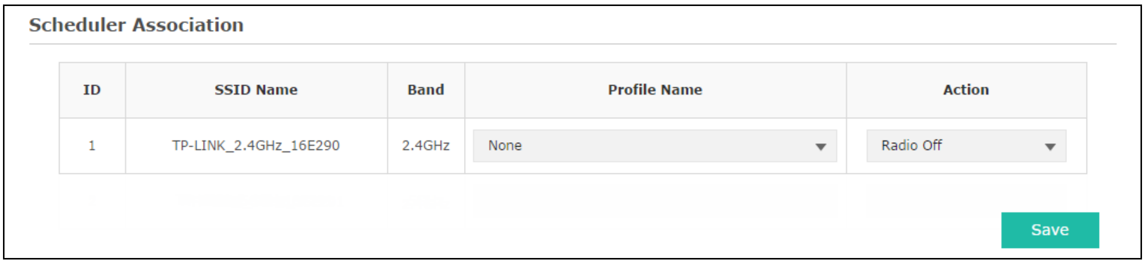
End Time: 18 : 00

Figure 7-27 Add a Rule

Scheduler Association

This zone will display different contents based on your selection of association mode in Settings.

1. Associated with SSID



Scheduler Association

ID	SSID Name	Band	Profile Name	Action
1	TP-LINK_2.4GHz_16E290	2.4GHz	None	Radio Off

Figure 7-28 Scheduler Association_Associated with SSID

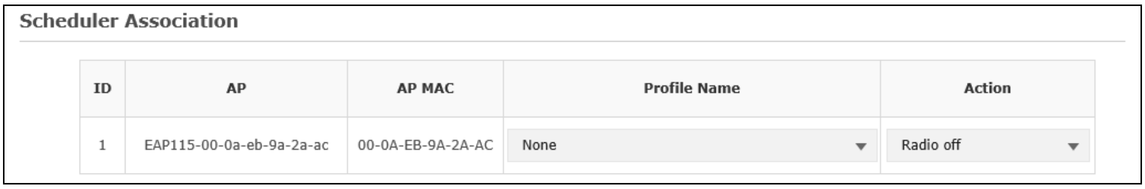
SSID Name: Displays the SSID of the standalone AP.

Band: Displays the frequency band which the wireless network operates at.

Profile Name: Select a profile name from the drop-down list. Profile name is configured in Scheduler Profile Configuration.

Action: Select **Radio On**/**Off** to turn on/off the wireless network during the time interval set for the profile.

2. Associated with AP



Scheduler Association

ID	AP	AP MAC	Profile Name	Action
1	EAP115-00-0a-eb-9a-2a-ac	00-0A-EB-9A-2A-AC	None	Radio off

Figure 7-29 Scheduler Association_Associated with AP

AP: Displays the name of the device.

AP MAC: Displays the MAC address of the device.

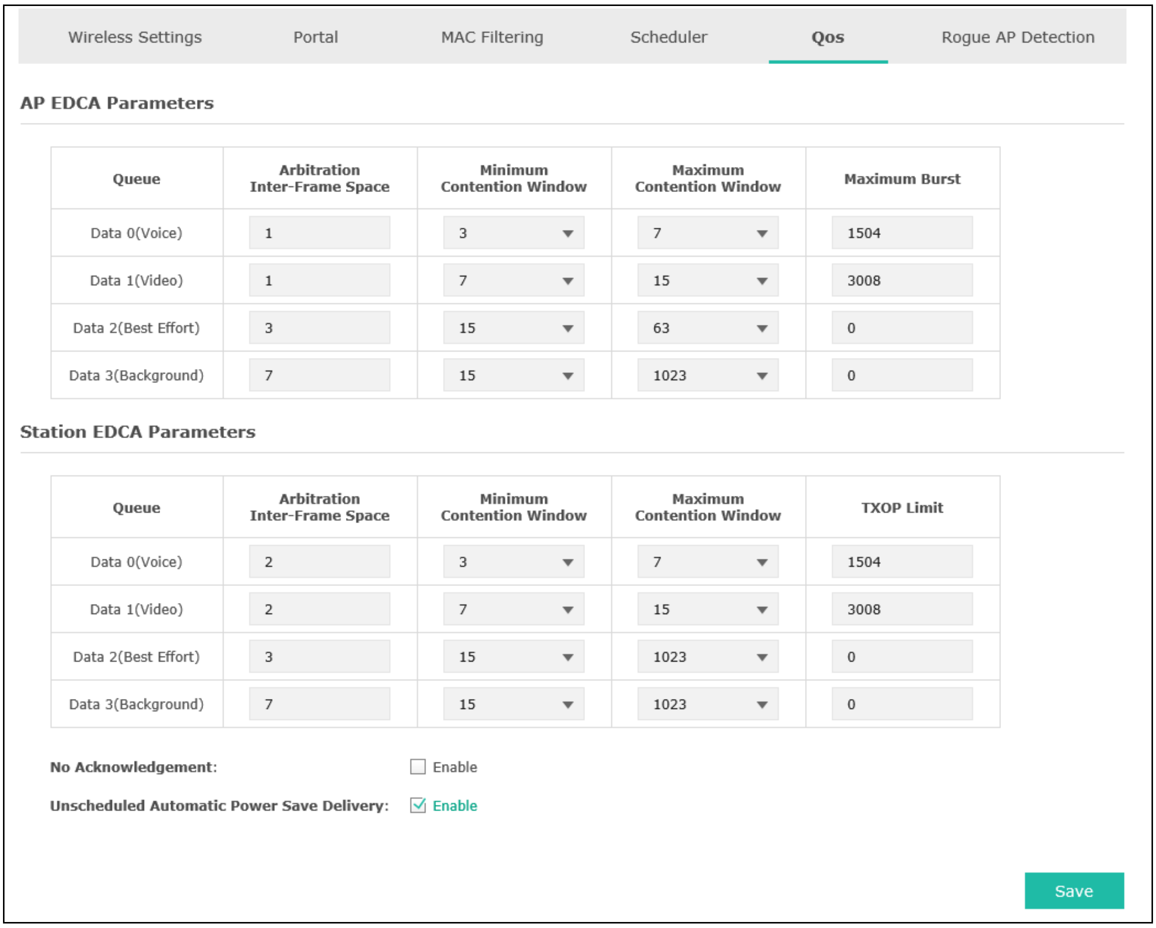
Profile Name: Select a profile name from the drop-down list. Profile name is configured in Scheduler Profile Configuration.

Action: Select **Radio On**/**Off** to turn on/off the wireless network during the time interval set for the profile.

7.2.5 QoS

The EAP supports Quality of Service (QoS) to prioritize voice and video traffic over other traffic types.

In normal use, the default values for the EAP device and station EDCA should not need to be changed. Changing these values affects the QoS provided.



AP EDCA Parameters

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

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

No Acknowledgement: ☐ Enable

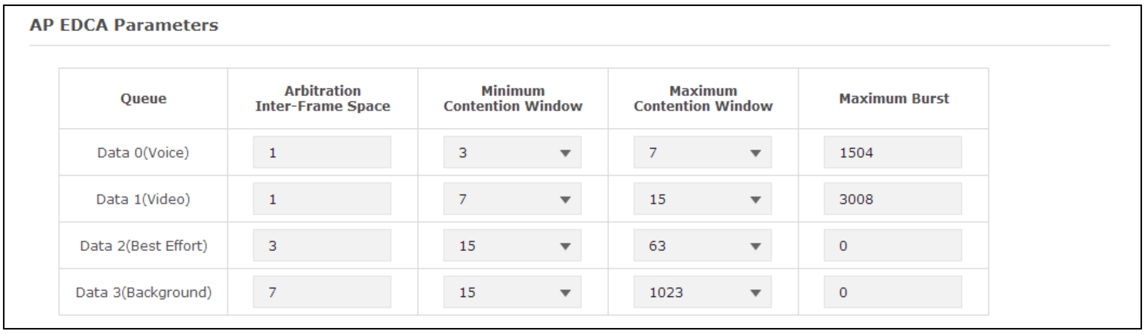
Unscheduled Automatic Power Save Delivery: ☑ Enable

Figure 7-30 QoS Page

Wi-Fi Multimedia (WMM):	By default, WMM is enabled. After WMM is enabled, the device has the QoS function to guarantee the transmission of audio and video packets with high priority.

7.2.5.1 AP EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) parameters affect traffic flowing from the EAP device to the client station.



AP EDCA Parameters

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

Figure 7-31 AP EDCA Parameters

Queue: Displays the transmission queues: Data 0>Data 1>Data 2>Data 3.

Arbitration Inter-Frame Space: A wait time for data frames. The wait time is measured in slots. Valid values for AIFS are from 1 to 15.

Minimum Contention Window: An input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.

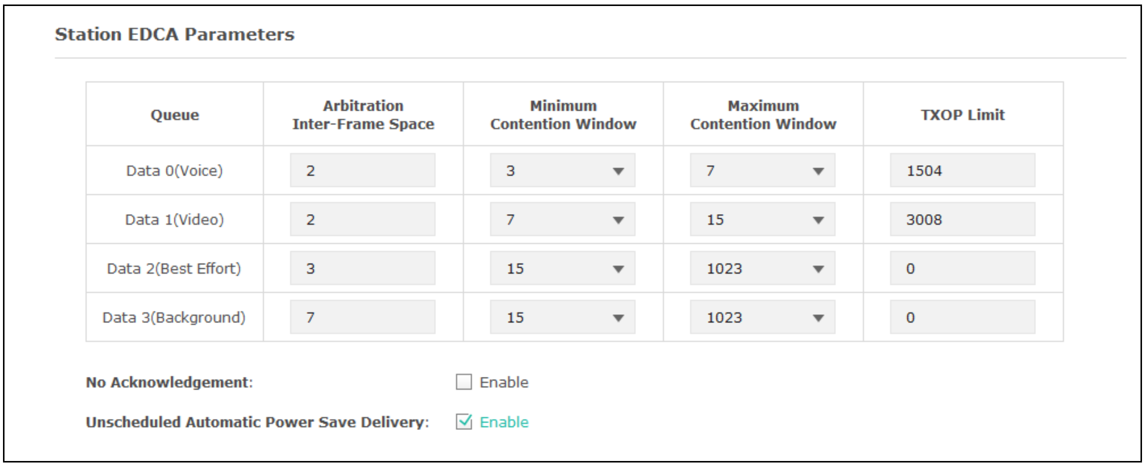
Maximum Contention Window: The upper limit (in milliseconds) for the doubling of the random backoff value.

Maximum Burst This parameter applies only to traffic flowing from EAP to the client station.

This value specifies (in milliseconds) 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. Valid values for Maximum Burst are from 0 to 8192 and should be exactly divided by 32.

7.2.5.2 Station EDCA Parameters

Station EDCA parameters affect traffic flowing from the client station to the EAP device.



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

No Acknowledgement: □ Enable

Unscheduled Automatic Power Save Delivery: ☑ Enable

Figure 7-32 Station EDCA Parameters

Queue: Displays the transmission queues: Data 0>Data 1>Data 2>Data 3.

Arbitration Inter-Frame Space: A wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 15.

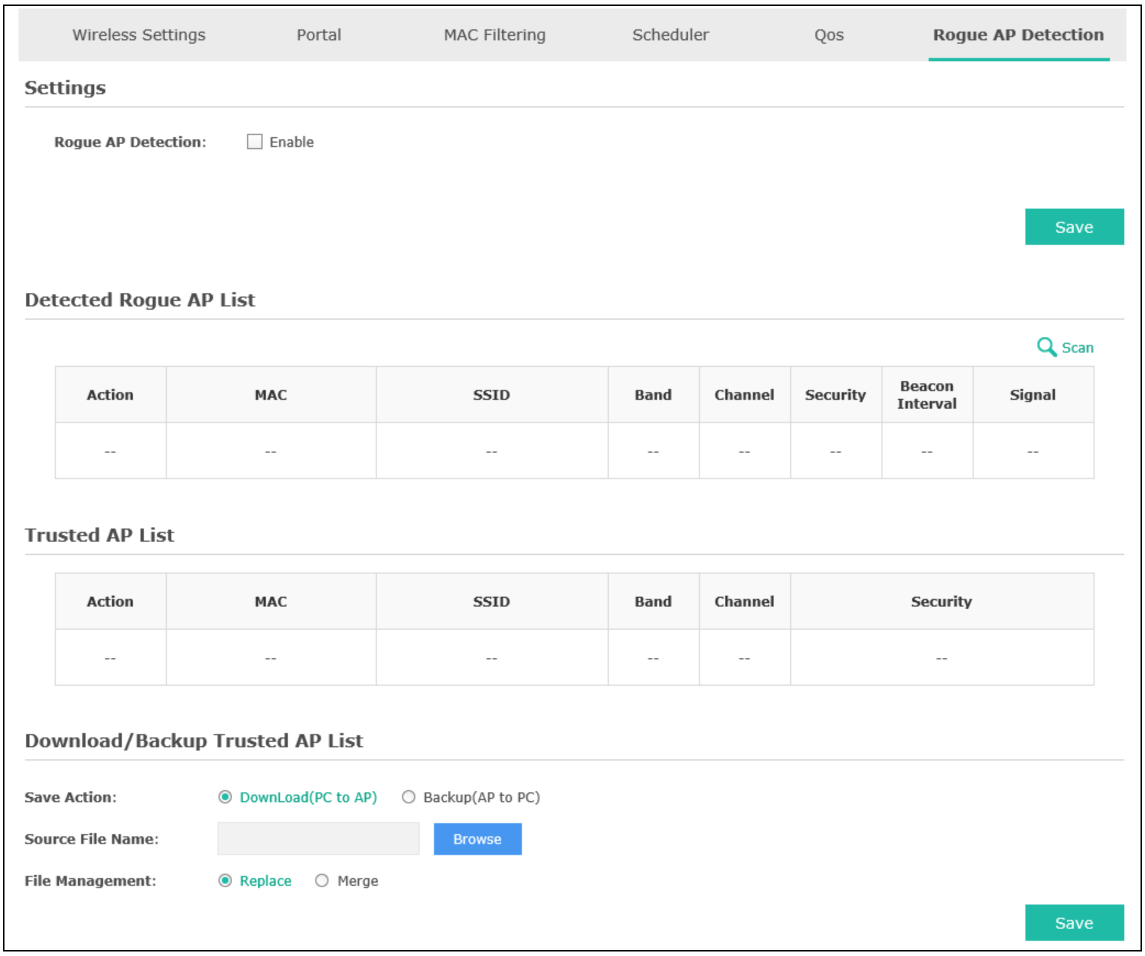
Minimum Contention Window: An input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.

Maximum Contention Window：	The upper limit (in milliseconds) for the doubling of the random backoff value.
TXOP Limit：	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 towards the EAP device. Valid values for TXOP Limit are from 0 to 8192 and should be exactly divided by 32.
No Acknowledgement：	Select **Enable** to specify that the EAP device should not acknowledge frames with QosNoAck as the service class value. By default, it is disabled.
Unscheduled Automatic Power Save Delivery：	Select **Enable** to enable APSD, which is a power management method. APSD is recommended if VoIP phones access the network through the EAP device. By default, it is enabled.

7.2.6 Rogue AP Detection

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator.

The EAP device can scan all channels to detect all APs in the vicinity of the network. If rogue APs are detected, they are shown on the Detected Rogue AP List. If an AP listed as a rogue is legitimate, you can add it to the Trusted AP List.



Settings

Rogue AP Detection: □ Enable

Detected Rogue AP List

Action	MAC	SSID	Band	Channel	Security	Beacon Interval	Signal
--	--	--	--	--	--	--	--

Trusted AP List

Action	MAC	SSID	Band	Channel	Security
--	--	--	--	--	--

Download/Backup Trusted AP List

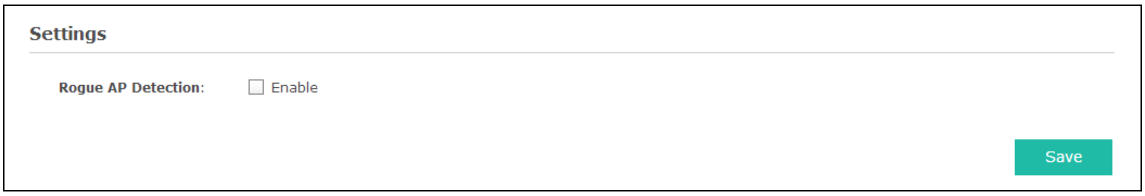
Save Action: ● DownLoad(PC to AP) ○ Backup(AP to PC)

Source File Name:

File Management: ● Replace ○ Merge

Figure 7-33 Rogue AP Detection Page

7.2.6.1 Settings



Settings

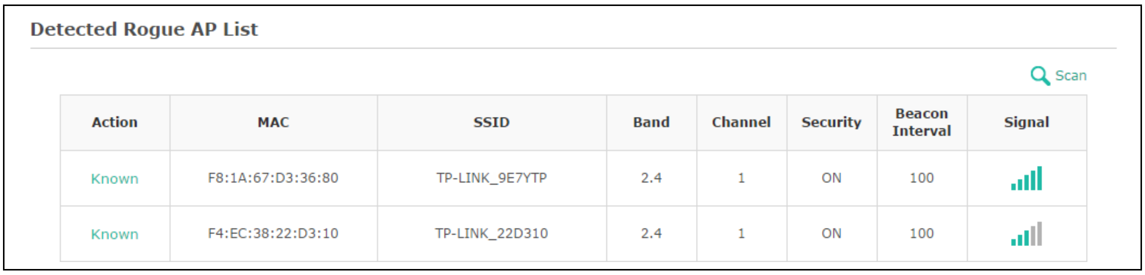
Rogue AP Detection: □ Enable

Figure 7-34 Enable Rogue AP Detection

Rogue AP Detection:	Check the box to enable Rogue AP Detection, then click **Save**.

7.2.6.2 Detected Rogue AP List

Information about the detected rogue APs is displayed in the list. By default, the status of the detected rogue AP is unknown. You can click **Known** in Action column to move the AP to the Trusted AP List.



Detected Rogue AP List

Scan

Action	MAC	SSID	Band	Channel	Security	Beacon Interval	Signal
Known	F8:1A:67:D3:36:80	TP-LINK_9E7YTP	2.4	1	ON	100	📶
Known	F4:EC:38:22:D3:10	TP-LINK_22D310	2.4	1	ON	100	📶

Figure 7-35 Detected Rogue AP List

Scan Click to scan rogue APs. Make sure you have enabled Rogue AP Detection and saved the setting before you click the button.

Action: Click **Known** to move the AP to the Trusted AP List. After the configurations are saved, the moved AP will not be displayed in the Detected Rogue AP List.

MAC: The MAC address of the rogue AP.

SSID: The SSID for the rogue AP.

Band: Displays the frequency band which the wireless network of the rogue AP operates at.

Channel: The channel on which the rogue AP is currently broadcasting.

Security: Displays the enabling or disabling of the security mode of the wireless network.

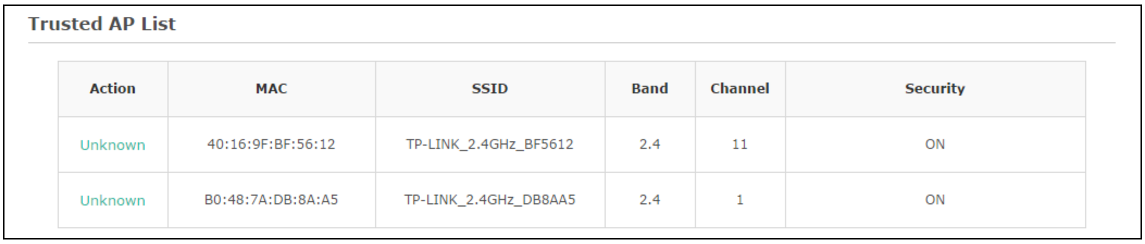
Beacon Interval: The beacon interval used by the rogue AP.

Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

Signal: The strength of the radio signal emitting from the rogue AP.

7.2.6.3 Trusted AP List

Information about the trusted APs is displayed in the list.



Trusted AP List

Action	MAC	SSID	Band	Channel	Security
Unknown	40:16:9F:BF:56:12	TP-LINK_2.4GHz_BF5612	2.4	11	ON
Unknown	B0:48:7A:DB:8A:A5	TP-LINK_2.4GHz_DB8AA5	2.4	1	ON

Figure 7-36 Trusted AP List

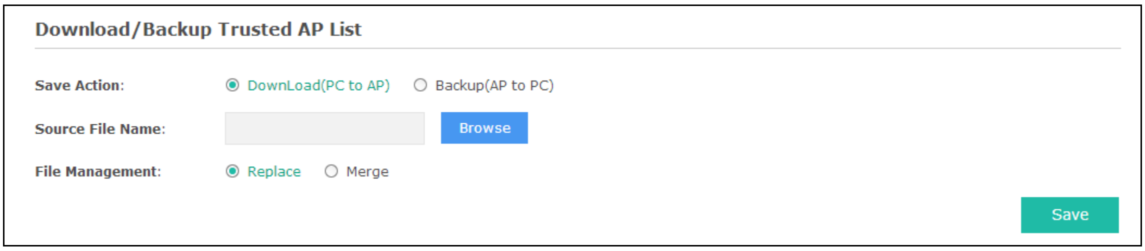
Action: Click **Unknown** to move the AP out of the Trusted AP List.

MAC:	The MAC address of the trusted AP.
SSID:	The SSID for the trusted AP.
Band:	Displays the frequency band which the wireless network of the trusted AP operates at.
Channel:	The channel on which the trusted AP is currently broadcasting.
Security:	Displays the enabling or disabling of the security mode of the wireless network.

7.2.6.4 Download/Backup Trusted AP List

You can import a list of trusted APs from a saved list which is acquired from another AP or created from a text file. The AP whose MAC address is in the Trusted AP List will not be detected as a rogue.

You can also backup a list and save it in your PC.



Download/Backup Trusted AP List

Save Action: ● DownLoad(PC to AP) ○ Backup(AP to PC)

Source File Name:

File Management: ● Replace ○ Merge

Figure 7-37 Download/Backup Trusted AP List

Save Action:	Select **Download (PC to AP)** to import a trusted AP list to the device. Select **Backup (AP to PC)** to copy the trusted AP list to your PC.
Source File Name:	Click **Browse** and choose the path of a saved trusted AP list or to save a trusted AP list.
File Management:	Select **Replace** to import the list and replace the contents of the Trusted AP List. Select **Merge** to import the list and add the APs in the imported file to the APs currently shown in the Trusted AP List

NOTE:

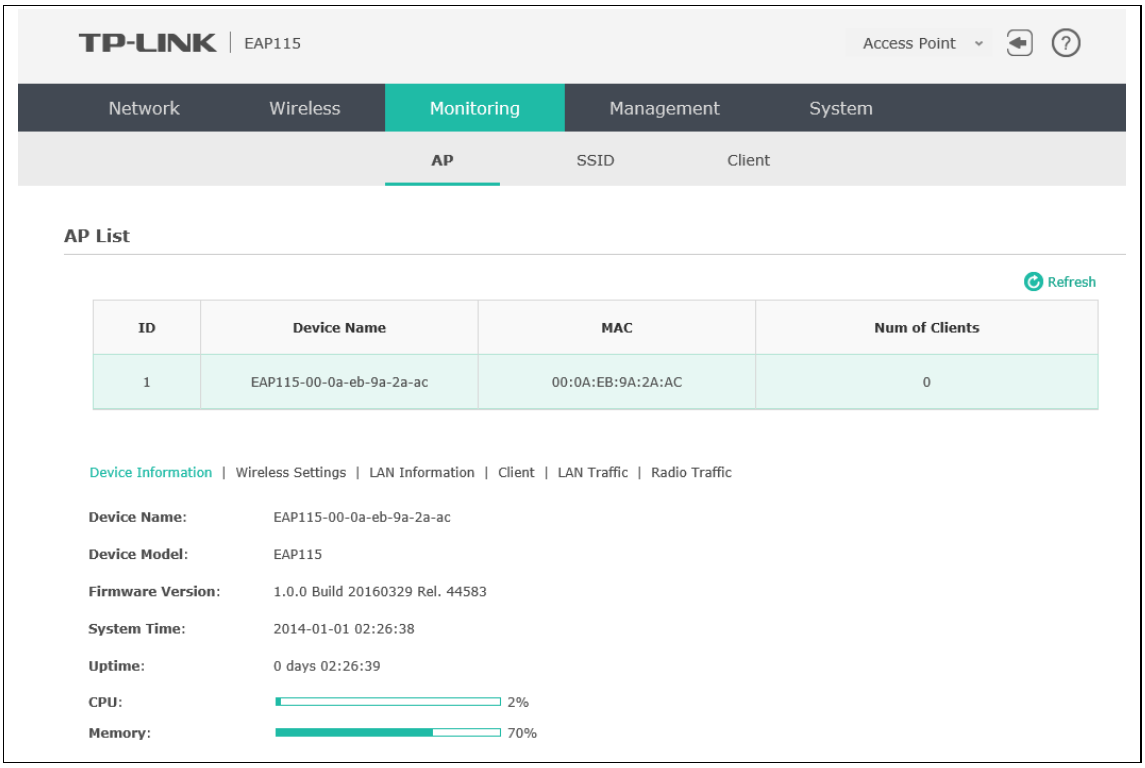
EAP device does not have any control over the APs in the Detected Rogue AP List.

7.3 Monitoring

On Monitoring page, you can monitor the network running status and statistics based on AP, SSID and Client.

7.3.1 AP

AP List on the Monitoring page displays the device name, its MAC address and the number of clients. Below the AP List the AP's detailed information will be shown, including Device Information, Wireless Settings, LAN Information, Client, LAN Traffic and Radio Traffic.



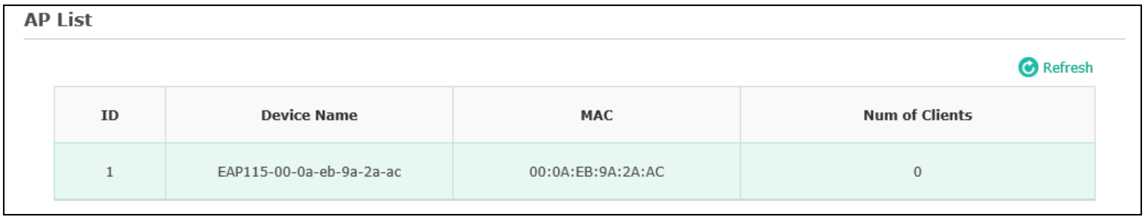
TP-LINK | EAP115
Access Point
Network
Wireless
Monitoring
Management
System
AP
SSID
Client
AP List
Refresh
Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

ID	Device Name	MAC	Num of Clients
1	EAP115-00-0a-eb-9a-2a-ac	00:0A:EB:9A:2A:AC	0

Device Name: EAP115-00-0a-eb-9a-2a-ac
Device Model: EAP115
Firmware Version: 1.0.0 Build 20160329 Rel. 44583
System Time: 2014-01-01 02:26:38
Uptime: 0 days 02:26:39
CPU: 2%
Memory: 70%

Figure 7-38 AP Monitoring

7.3.1.1 AP List



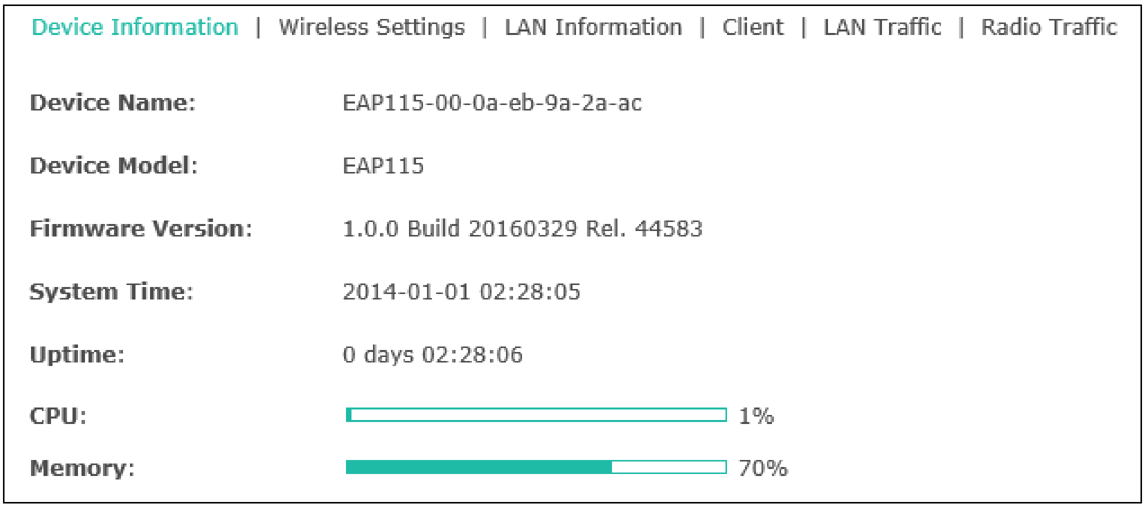
ID	Device Name	MAC	Num of Clients
1	EAP115-00-0a-eb-9a-2a-ac	00:0A:EB:9A:2A:AC	0

Figure 7-39 AP List

Device Name: Displays the device name.

MAC:	Displays the MAC address of the EAP.
Num of Clients:	Displays the number of clients connected to the EAP.

- ## Device Information


Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Device Name: EAP115-00-0a-eb-9a-2a-ac

Device Model: EAP115

Firmware Version: 1.0.0 Build 20160329 Rel. 44583

System Time: 2014-01-01 02:28:05

Uptime: 0 days 02:28:06

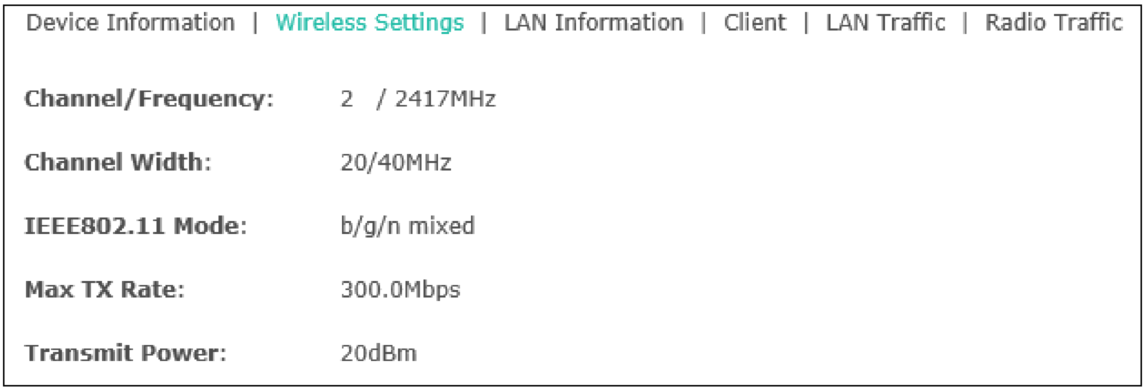
CPU: 1%

Memory: 70%

Figure 7-40 Device Information

Device Name:	Displays the device name.
Device Model:	Displays the model of the device.
Firmware Version:	Displays the firmware version of the device. If you want to upgrade the firmware, please refer to 8.5 Firmware Upgrade.
System Time:	Displays the system time of the device. If you want to adjust the system time, please refer to 8.2.1 Time Settings.
Uptime:	Displays the time that has elapsed since the last reboot.
CPU:	Displays the CPU occupancy, which helps you to preliminarily judge whether the device functions properly.
Memory:	Displays the memory usage , which helps you to preliminarily judge whether the device functions properly.

- ## Wireless Settings



Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Channel/Frequency: 2 / 2417MHz

Channel Width: 20/40MHz

IEEE802.11 Mode: b/g/n mixed

Max TX Rate: 300.0Mbps

Transmit Power: 20dBm

Figure 7-41 Wireless Settings

Channel/Frequency: Displays the channel number and the operating frequency. If you want to change them, please refer to 5.1.1 Wireless Basic Settings.

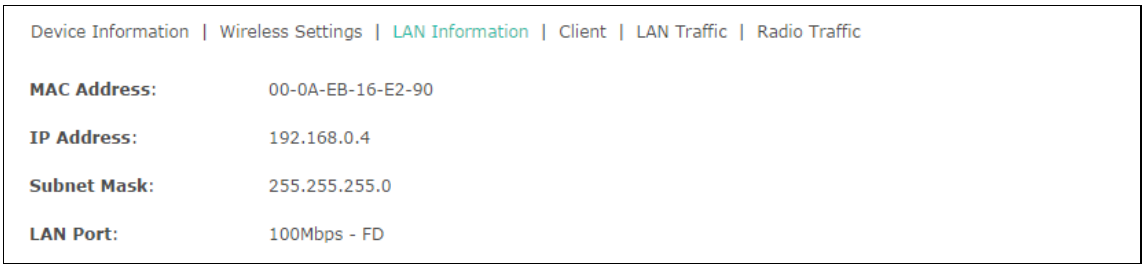
Channel Width: Displays the spectral width of the radio channel used by the device. If you want to change it, refer to 5.1.1 Wireless Basic Settings.

IEEE802.11 Mode: Displays the radio standard used for operation of your device. If you want to change it, refer to 5.1.1 Wireless Basic Settings.

Max TX Rate: Displays the maximum data rate at which the device should transmit wireless packets.

Transmit Power: Displays the maximum average transmit power of the device. If you want to change it, refer to 5.1.1 Wireless Basic Settings.

- ## LAN Information



Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

MAC Address: 00-0A-EB-16-E2-90

IP Address: 192.168.0.4

Subnet Mask: 255.255.255.0

LAN Port: 100Mbps - FD

Figure 7-42 LAN Information

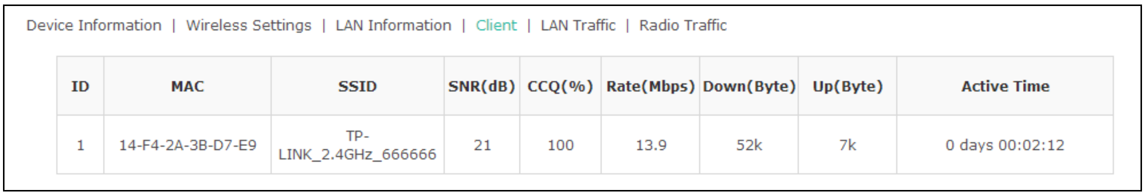
MAC Address: Displays the MAC address of the device.

IP Address: Displays the IP address of the device.

Subnet Mask: Displays the subnet mask of the device.

LAN Port: Displays the maximum transmission rate and duplex mode (half-duplex or full-duplex) of the port.

- ## Client


Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

ID	MAC	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time
1	14-F4-2A-3B-D7-E9	TP-LINK_2.4GHz_666666	21	100	13.9	52k	7k	0 days 00:02:12

Figure 7-43 Client

MAC: Displays the MAC address of the client of the AP selected in AP List.

SSID: Displays the SSID the client is connected to.

SNR(dB): Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. The bigger the value of SNR, the better network performance the device provides.

CCQ(%): Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.

Rate(Mbps): Displays the data rate at which the client transmits wireless packets.

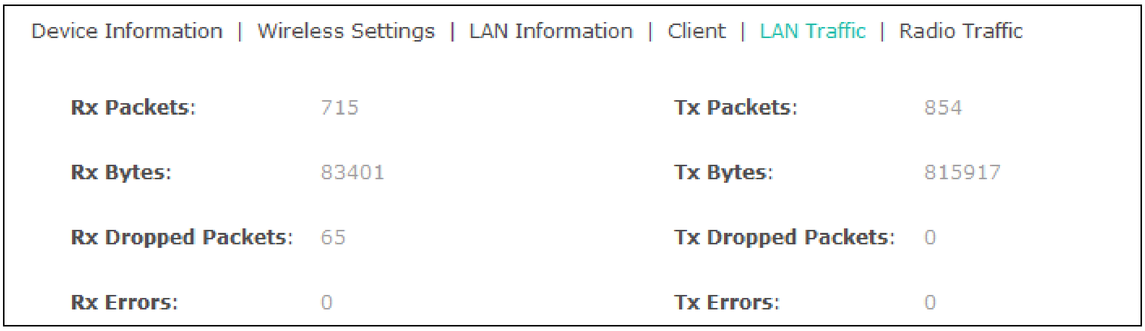
Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

Active Time: Displays the amount of time the client has been connected to the device.

- ## LAN Traffic

Click **LAN Traffic** and you can monitor the data transmission status of the LAN port.


Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Rx Packets: 715
Tx Packets: 854
Rx Bytes: 83401
Tx Bytes: 815917
Rx Dropped Packets: 65
Tx Dropped Packets: 0
Rx Errors: 0
Tx Errors: 0

Figure 7-44 LAN Traffic

Rx/Tx Packets: Displays the total amount of packets received/sent on the LAN port.

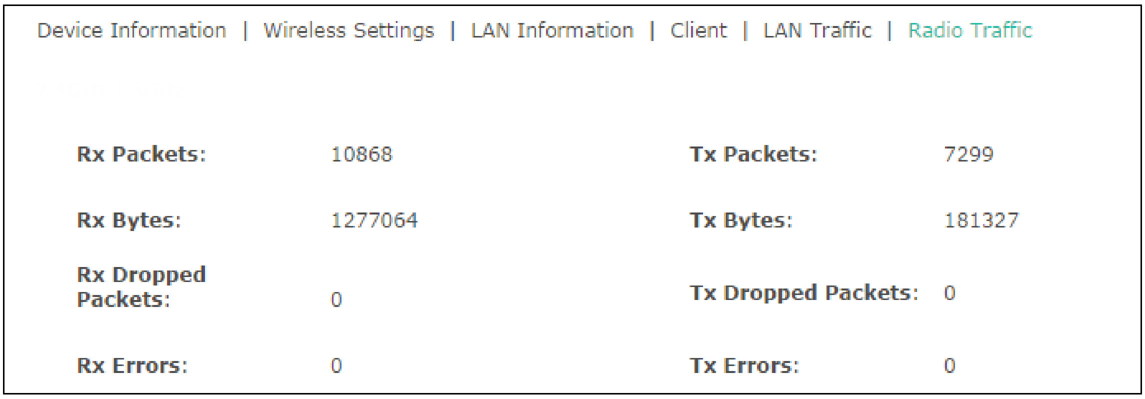
Rx/Tx Bytes: Displays the total amount of data (in bytes) received/sent on the LAN port.

Rx/Tx Dropped Packets: Displays the total amount of dropped packets received/sent on the LAN port.

Rx/Tx Errors:	Displays the total amount of error packets received/sent-on the LAN port.

- ## Radio Traffic

Click **Radio Traffic** and you can monitor the data transmission status of the wireless network.



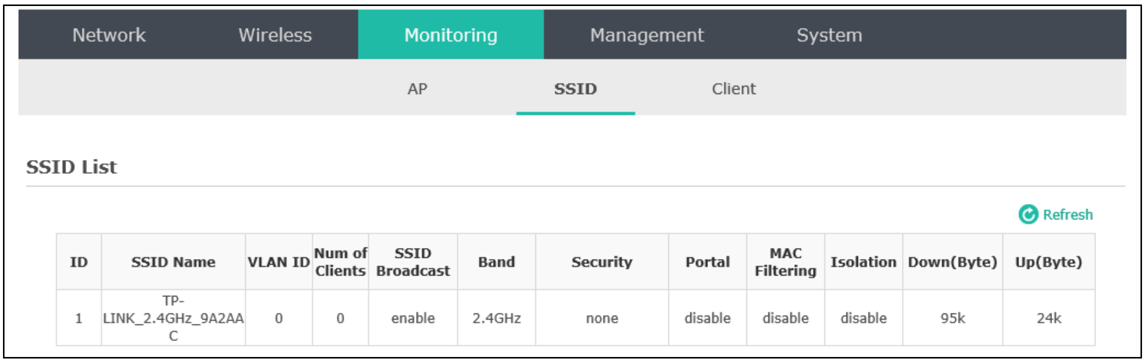
Device Information | Wireless Settings | LAN Information | Client | LAN Traffic | Radio Traffic

Rx Packets:	10868	Tx Packets:	7299
Rx Bytes:	1277064	Tx Bytes:	181327
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

Figure 7-45 Radio Traffic

Rx/Tx Packets:	Displays the total amount of packets received/sent by the wireless network.
Rx/Tx Bytes:	Displays the total amount of data (in bytes) received/sent by the wireless network.
Rx/Tx Dropped Packets:	Displays the total amount of dropped packets received/sent by the wireless network.
Rx/Tx Errors:	Displays the total amount of error packets received/sent by the wireless network.

7.3.2 SSID

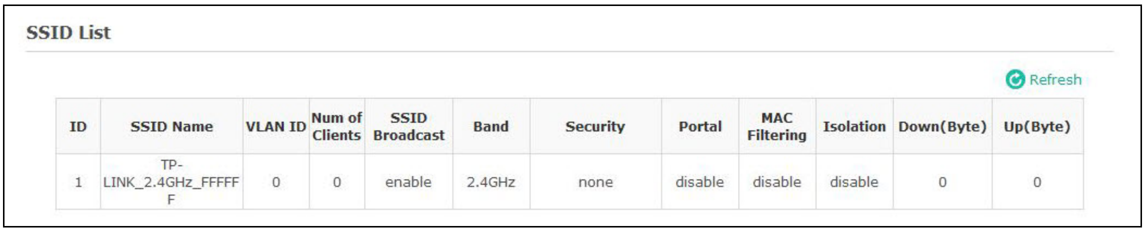


ID	SSID Name	VLAN ID	Num of Clients	SSID Broadcast	Band	Security	Portal	MAC Filtering	Isolation	Down(Byte)	Up(Byte)
1	TP-LINK_2.4GHz_9A2AAC	0	0	enable	2.4GHz	none	disable	disable	disable	95k	24k

Figure 7-46 SSID Monitoring

7.3.2.1 SSID List

In SSID List you can monitor the related parameters of the wireless network.


SSID List

ID	SSID Name	VLAN ID	Num of Clients	SSID Broadcast	Band	Security	Portal	MAC Filtering	Isolation	Down(Byte)	Up(Byte)
1	TP-LINK_2.4GHz_FFFFFF	0	0	enable	2.4GHz	none	disable	disable	disable	0	0

Figure 7-47 SSID List

SSID Name: Displays the SSID name. If you want to modify it, please refer to 7.2.1.2 SSIDs.

VLAN ID: Displays the VLAN which the SSID belongs to. If you want to change the VLAN ID, please refer to 7.2.1.2 SSIDs.

Num of Clients: Displays the number of clients connected to the SSID. If you want to get more information about these clients, please refer to 7.2.1.2 SSIDs.

SSID Broadcast: Displays the enabling or disabling of SSID broadcast. If you want to modify it, please refer to 7.2.1.2 SSIDs.

Band: Displays the frequency band the wireless network is operating at.

Security: Displays the security mode the wireless network is applying. If you want to modify it, please refer to 7.2.1.2 SSIDs.

Portal: Displays the enabling or disabling of Portal. If you want to modify it, please refer to 7.2.1.2 SSIDs.

MAC Filtering: Displays the enabling or disabling of MAC Filtering. If you want to modify it, please refer to 7.2.1.2 SSIDs.

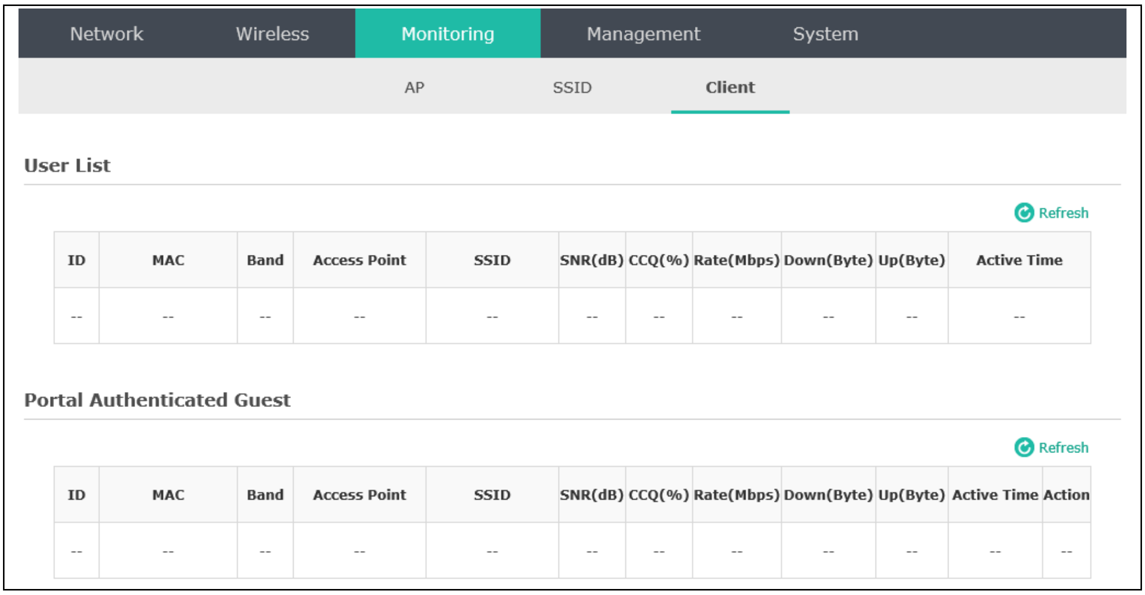
Isolation: Displays the enabling or disabling of SSID Isolation. If you want to modify it, please refer to 7.2.1.2 SSIDs.

Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

7.3.3 Client

From User List, you can monitor the status of all the clients connected to the EAP including those who are authenticated.



User List

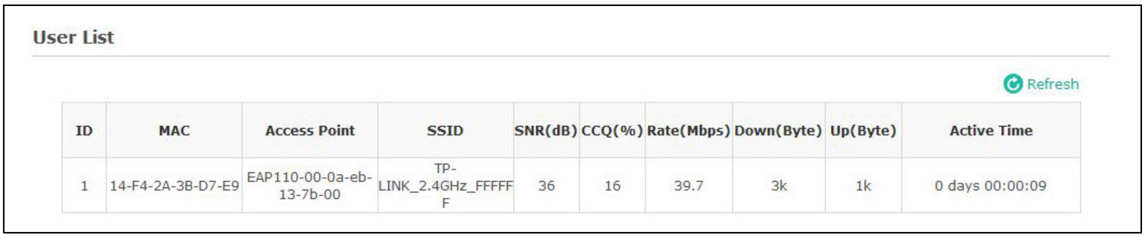
ID	MAC	Band	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time
--	--	--	--	--	--	--	--	--	--	--

Portal Authenticated Guest

ID	MAC	Band	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time	Action
--	--	--	--	--	--	--	--	--	--	--	--

Figure 7-48 Client Monitoring

7.3.3.1 User List



User List

ID	MAC	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(Byte)	Up(Byte)	Active Time
1	14-F4-2A-3B-D7-E9	EAP110-00-0a-eb-13-7b-00	TP-LINK_2.4GHz_FFFFF F	36	16	39.7	3k	1k	0 days 00:00:09

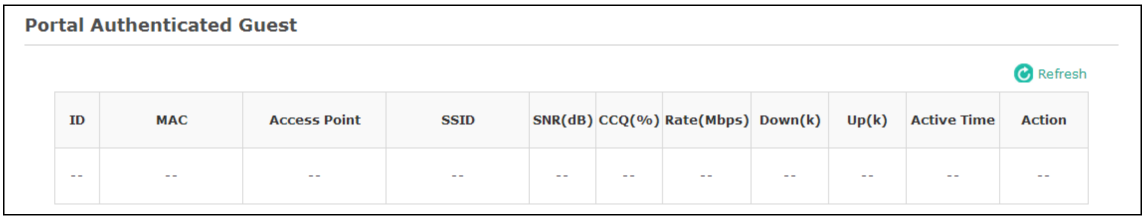
Figure 7-49 User List

MAC:	Displays the MAC address of the client.
Access Point:	Displays the name of the device to which the client is connected.
SSID:	Displays the SSID the client is connected to.
SNR(dB):	Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. The bigger the value of SNR, the better network performance the device provides.
CCQ(%):	Displays the wireless Client Connection Quality (CCQ). CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.
Rate(Mbps):	Displays the data rate at which the client transmits wireless packets.
Down(Byte):	Displays the throughput of the downstream data.
Up(Byte):	Displays the throughput of the upstream data.

Active Time: Displays the amount of time the client has been connected to the device.

7.3.3.2 Portal Authenticated Guest

The Portal Authenticated Guest displays information about clients that have set up valid authentication.



Portal Authenticated Guest

Refresh

ID	MAC	Access Point	SSID	SNR(dB)	CCQ(%)	Rate(Mbps)	Down(k)	Up(k)	Active Time	Action
--	--	--	--	--	--	--	--	--	--	--

Figure 7-50 Portal Authenticated Guest

MAC: Displays the MAC address of the authenticated client.

Access Point: Displays the name of the device to which the authenticated client is connected

SSID: Displays the SSID the authenticated client is connected to.

SNR(dB): Signal to Noise Ratio, the power ratio between the received wireless signal strength and the environmental noise strength. The bigger the value of SNR, the better network performance the device provides.

CCQ(%): Displays the Client Connection Quality (CCQ) of the authenticated client. CCQ refers to the ratio of current effective transmission bandwidth and the theoretically maximum available bandwidth. CCQ reflects the actual link condition.

Rate(Mbps): Displays the data rate at which the authenticated client transmits wireless packets.

Down(Byte): Displays the throughput of the downstream data.

Up(Byte): Displays the throughput of the upstream data.

Active Time: Displays the amount of time the authenticated client has been connected to the root AP.

Action: Click **Unauthorize** to stop giving authorization to the clients connected to the wireless network.

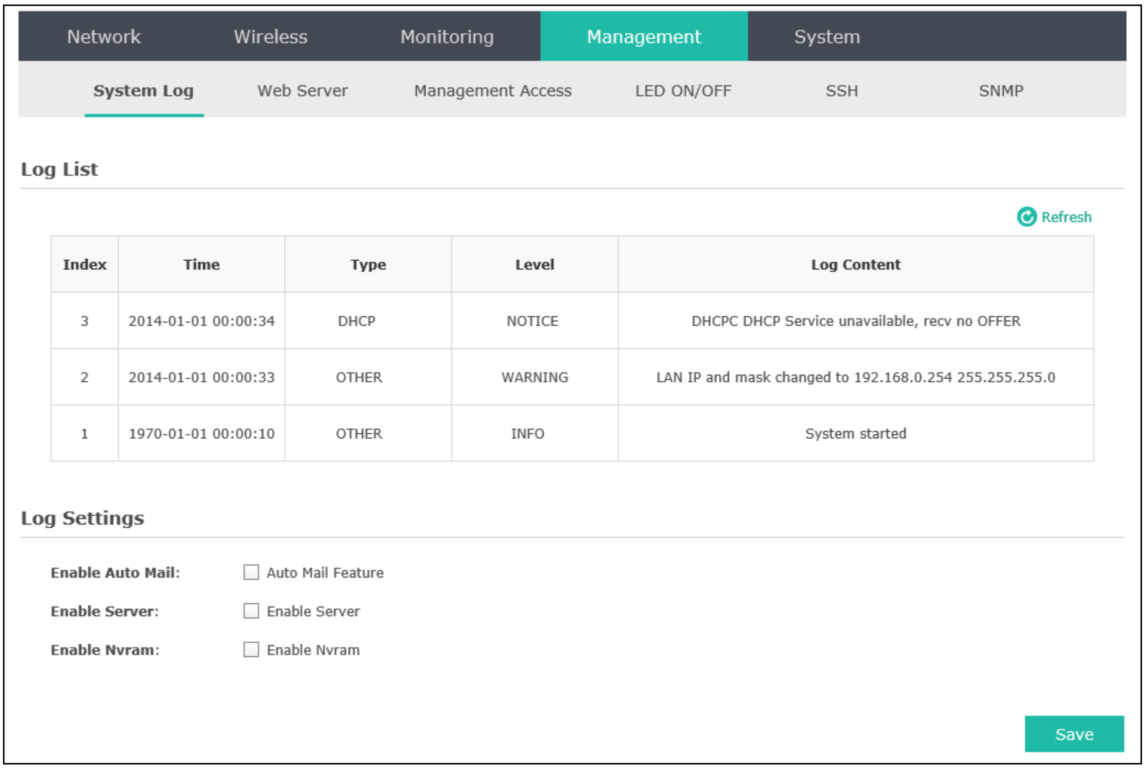
7.4 Management

Management page is mainly used for device management and maintenance.

7.4.1 System Log

System log records information about hardware, software as well as system issues and monitors system events. With the help of system log, you can get informed of system running status and detect the reasons for failure.

Following is the page of System Log.



Log List

Index	Time	Type	Level	Log Content
3	2014-01-01 00:00:34	DHCP	NOTICE	DHCPC DHCP Service unavailable, recv no OFFER
2	2014-01-01 00:00:33	OTHER	WARNING	LAN IP and mask changed to 192.168.0.254 255.255.255.0
1	1970-01-01 00:00:10	OTHER	INFO	System started

Log Settings

Enable Auto Mail: ☐ Auto Mail Feature

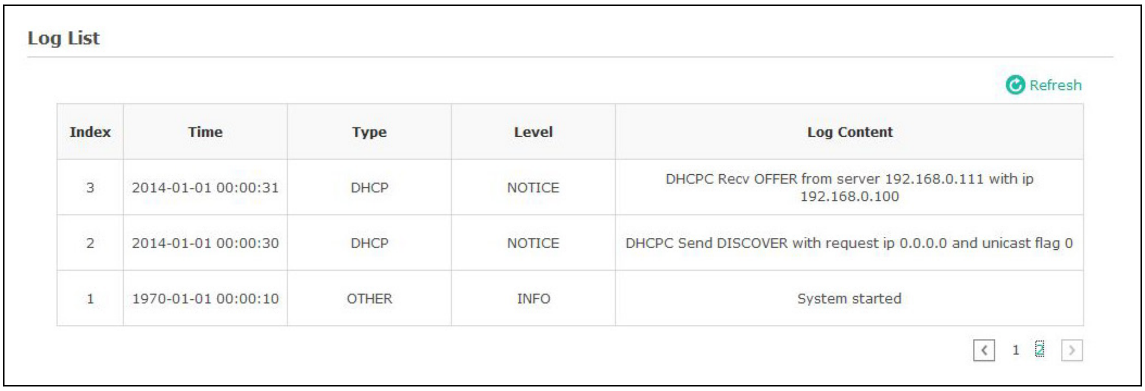
Enable Server: ☐ Enable Server

Enable Nvram: ☐ Enable Nvram

Figure 7-51 System Log Page

7.4.1.1 Log List

From Log List you can view detailed information about hardware, software, system issues and so on.



Log List

Refresh

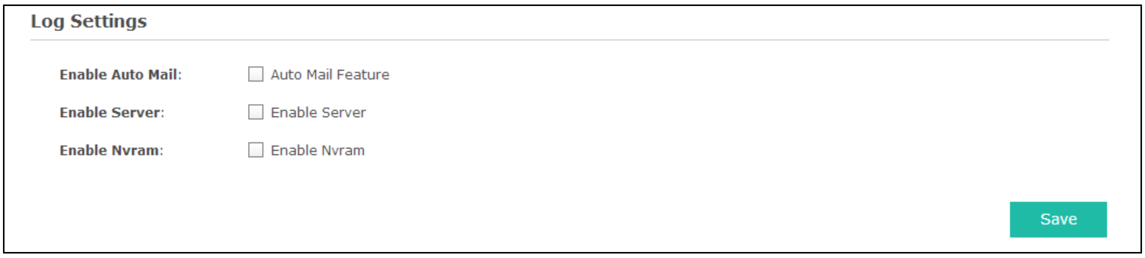
Index	Time	Type	Level	Log Content
3	2014-01-01 00:00:31	DHCP	NOTICE	DHCPC Recv OFFER from server 192.168.0.111 with ip 192.168.0.100
2	2014-01-01 00:00:30	DHCP	NOTICE	DHCPC Send DISCOVER with request ip 0.0.0.0 and unicast flag 0
1	1970-01-01 00:00:10	OTHER	INFO	System started

< 1 2 >

Figure 7-52 Log List

7.4.1.2 Log Settings

You can choose the way to receive system logs in Log Settings zone, where these parameters can be configured: Enable Auto Mail, Enable Server and Enable Nvram.



Log Settings

Enable Auto Mail: □ Auto Mail Feature

Enable Server: □ Enable Server

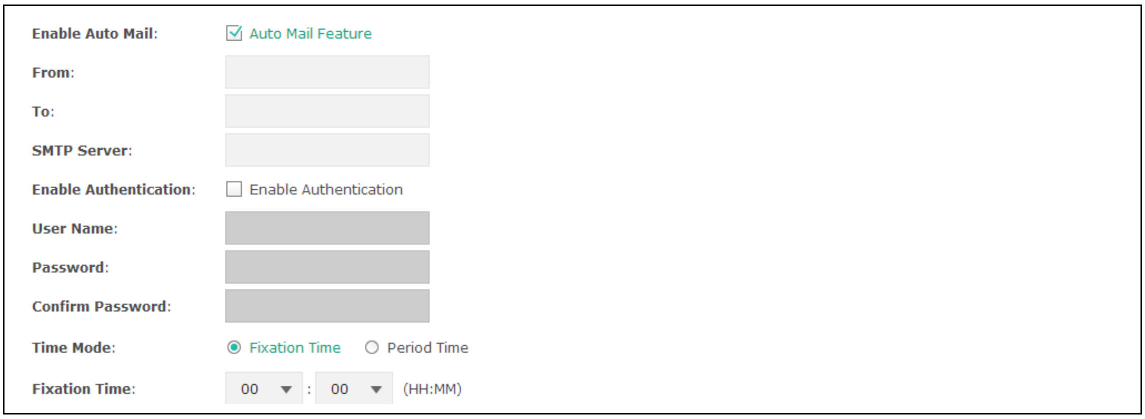
Enable Nvram: □ Enable Nvram

Save

Figure 7-53 Log Settings

- **Enable Auto Mail**

If Auto Mail is enabled, system logs will be sent to a mailbox. The following content will be shown.



Enable Auto Mail: ☑ Auto Mail Feature

From:

To:

SMTP Server:

Enable Authentication: □ Enable Authentication

User Name:

Password:

Confirm Password:

Time Mode: ● Fixation Time ○ Period Time

Fixation Time: 00 ▼ : 00 ▼ (HH:MM)

Figure 7-54 Enable Auto Mail

From: Enter the sender's email address.

To: Enter the recipient's email address, which will receive the system logs.

SMTP Server: Enter the IP address of the SMTP server.

Enable Authentication: Generally users are required to log in to the SMTP server by entering user name and password.

- **User Name**: Enter the sender's email address.
- **Password**: Enter the password of the sender's email address.
- **Confirm Password**: Enter the password again for confirmation.

Time Mode: System logs can be sent at specific time or time interval.

- **Fixation Time**: Set a fixed time, for example, 15:00. The recipient will receive the system logs sent by the device at 15:00 every day.
- **Period Time**: Set a time interval, for example, 5 hours. The recipient will receive the system logs sent by the device every 5 hours.

- ## Enable Server

System logs can also be sent to a server. After Auto Mail Feature is enabled, the following content will be shown.

Enable Server: ☑ Enable Server

System Log Server IP: 0.0.0.0

System Log Server Port: 514

Figure 7-55 Enable Server

System Log Server IP: Enter the IP address of the remote server.

System Log Server Port: Enter the port of the remote server.

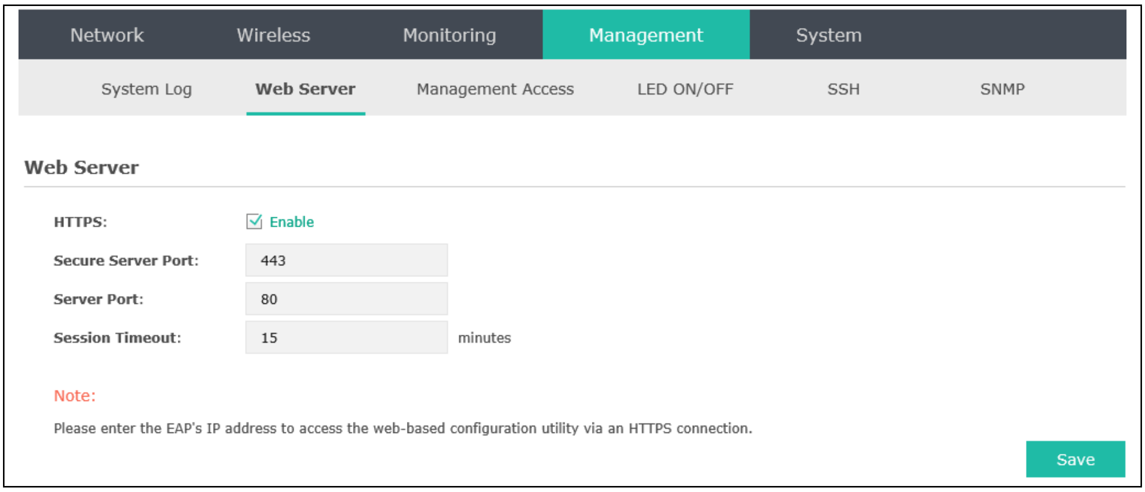
- ## Enable Nvram

By default, Nvram is disabled. Check the box to enable Nvram, system logs will be saved after power supply is cut.

7.4.2 Web Server

You can log in web management interface, thereby manage and maintain the device.

Following is the page of Web Server.



Web Server

HTTPS: ☑ Enable

Secure Server Port: 443

Server Port: 80

Session Timeout: 15 minutes

Note:

Please enter the EAP's IP address to access the web-based configuration utility via an HTTPS connection.

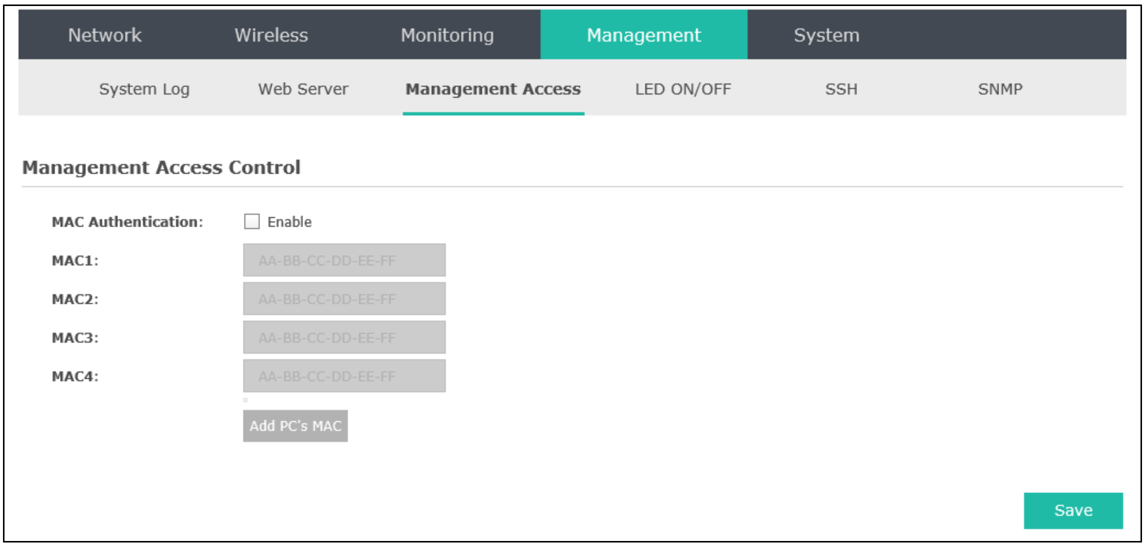
Figure 7-56 Web Server Page

HTTPS:	HTTPS (Hypertext Transfer Protocol Secure) is enabled by default.
Secure Server Port:	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
Server Port:	Designate a server port for web server in HTTP mode. By default the port is 80.
Session Timeout:	Set the session timeout time. If you do nothing with the web management page within the timeout time, the system will log out automatically. Please login again if you want to go back to web management page.

7.4.3 Management Access

Management Access Control allows you to configure up to four MAC addresses of the hosts that are allowed to log in to the web management page of the EAP. Click **Add PC's MAC** and the MAC address of the current host will be added to MAC address list.

Following is the page of Management Access.



Management Access Control

MAC Authentication: □ Enable

MAC1: AA-BB-CC-DD-EE-FF

MAC2: AA-BB-CC-DD-EE-FF

MAC3: AA-BB-CC-DD-EE-FF

MAC4: AA-BB-CC-DD-EE-FF

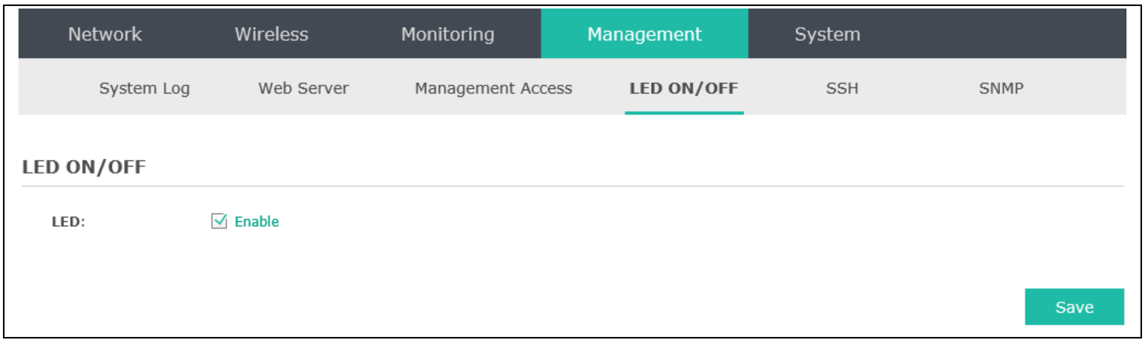
Figure 7-57 Management Access Page

MAC Authentication: Check the box to enable MAC Authentication. After MAC Authentication is enabled, only the PCs in MAC address list can log in the device's web management page. By default this function is disabled. All PCs in LAN can log in and manage the device.

MAC1~MAC4: Enter the MAC addresses of the PCs which are authorized to log in the device.

7.4.4 LED ON/OFF

Following is the page of LED ON/OFF. By default the LED is on.



LED ON/OFF

LED: ☑ Enable

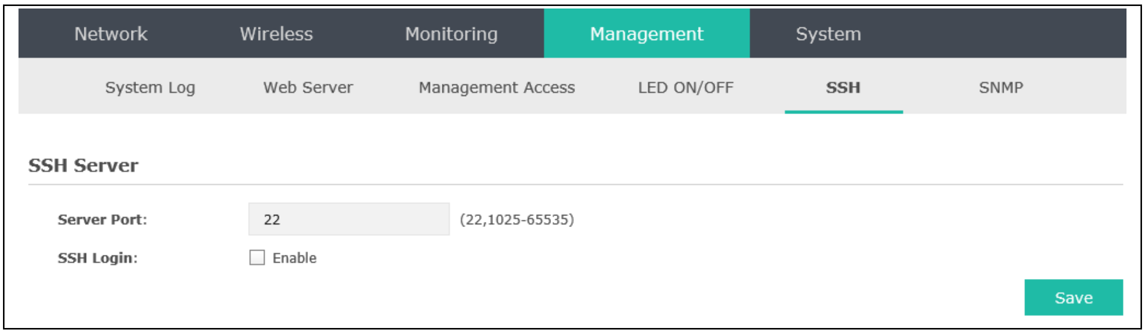
Figure 7-58 LED ON/OFF

7.4.5 SSH

This device supports the SSH Server function that allows users to login and manage it through SSH connection on the SSH client software.

SSH (Secure Shell) is a security protocol established on application and transport layers. SSH-encrypted-connection is similar to a telnet connection, but essentially the old telnet remote management method is not safe, because the password and data transmitted with plain-text can be easily intercepted. SSH can provide information security and powerful authentication when you login this device remotely through an insecure network environment. It can encrypt all the transmission data and prevent the information in remote management from being leaked.

Following is the page of SSH.



SSH Server

Server Port: 22 (22,1025-65535)

SSH Login: □ Enable

Figure 7-59 SSH Page

Server Port:	Enter the server port. By default, it is port 22.
SSH Login:	Check the box to enable SSH Server. By default, it is disabled.

7.4.6 SNMP

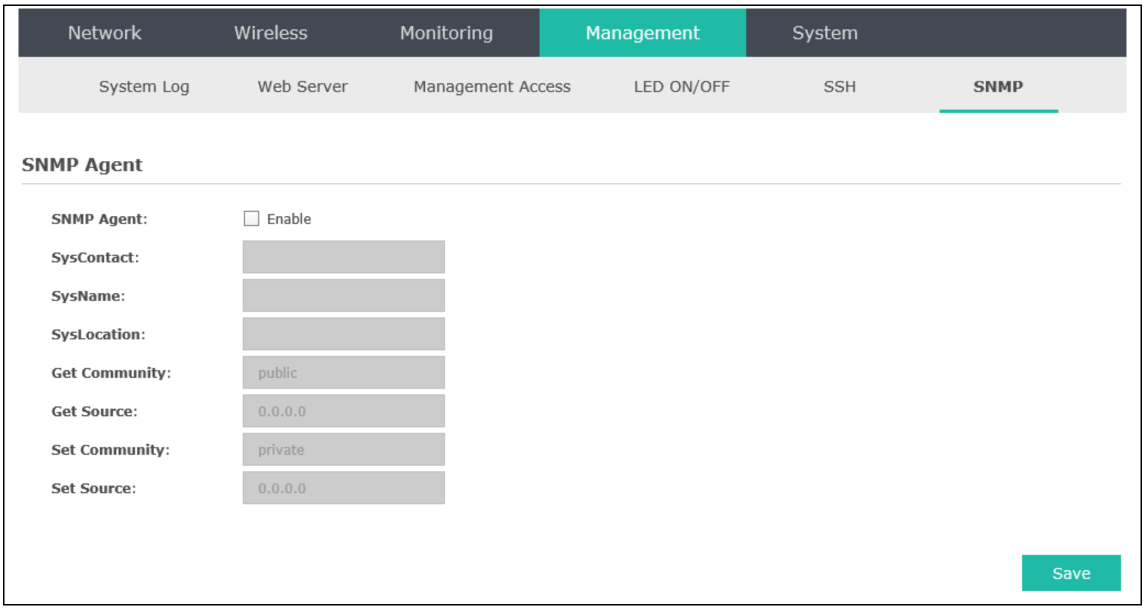
The device can be configured as an SNMP agent.

SNMP (Simple Network Management Protocol), the most widely applied network management protocol, provides a management framework to monitor and maintain Internet devices. Main functions of SNMP include monitoring network performance, detecting and analyzing network error, configuring network devices, and so on. When networks function properly, SNMP can perform the functions of statistics, configuration and testing. When networks have troubles, SNMP can detect and restore these troubles.

An SNMP consists of three key components: manager, agent and MIB (Management Information Base). SNMP manager is a client program operating at workstation, assisting network administrators to accomplish most network device management tasks. An agent is a network-management software module that resides on a managed device and responsible for receiving and dealing with data sent by managing device. Generally the managed devices are network devices including hosts, bridges, switches and routers. MIB is the collection of managed devices. It defines a series of properties of the managed devices. Every SNMP agent has its own MIB.

Once the device has become an SNMP agent, it is able to receive and process request messages from SNMP manager.

Following is the page of SNMP.



SNMP Agent

SNMP Agent: □ Enable

SysContact:

SysName:

SysLocation:

Get Community: public

Get Source: 0.0.0.0

Set Community: private

Set Source: 0.0.0.0

Figure 7-60 SNMP Page

SNMP Agent: Enable SNMP Agent and the SNMP Agent will collect the information of this device and respond to information requests from one or more management systems.

SysContact: Enter the textual identification of the contact person for this managed node.

SysName: Enter an administratively-assigned name for this managed node.

SysLocation: Enter the physical location of this managed node.

Get Community: Community refers to a host group aiming at network management. Get Community only has the read-only right of the device's SNMP information. The community name can be considered a group password. The default setting is public.

Get Source: Defines the IP address (for example, 10.10.10.1) or subnet for management systems that can serve as Get Community to read the SNMP information of this device. The format of subnet is “IP address/bit” (such as 10.10.10.0/24). The default is 0.0.0.0, which means all hosts can read the SNMP information of this device.

Set Community: Set Community has the read and write right of the device's SNMP information. Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered a group password. The default setting is private.

Set Source: Defines the IP address (for example, 10.10.10.1) or subnet for management systems that can serve as Set Community to read and write the SNMP information of this device. The format of subnet is “IP address/bit” (such as 10.10.10.0/24). The default is 0.0.0.0, which means all hosts can read and write the SNMP information of this device.

NOTE:

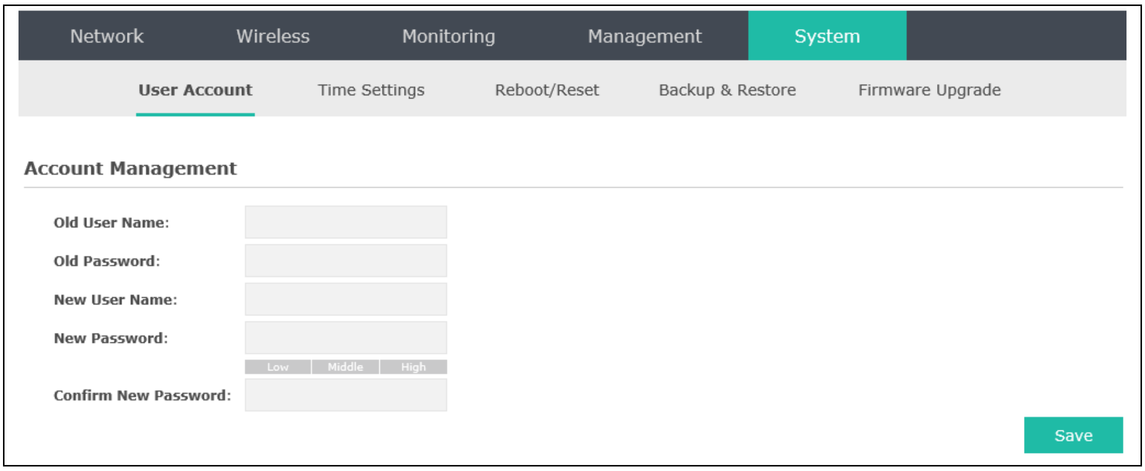
Defining community can allow management systems in the same community to communicate with the SNMP Agent. The community name can be seen as the shared password of the network hosts group. Thus, for the security, we suggest modifying the default community name before enabling the SNMP Agent service. If the field of community is blank, the SNMP Agent will not respond to any community name.

7.5 System

System page is mainly used to configure some basic information like user account and time, and realize functions including reboot, reset, backup, restore and upgrade the device.

7.5.1 User Account

You can change the username and password to protect your device from unauthorized login. We recommend that you change the default user password on the very first system setup.



Account Management

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

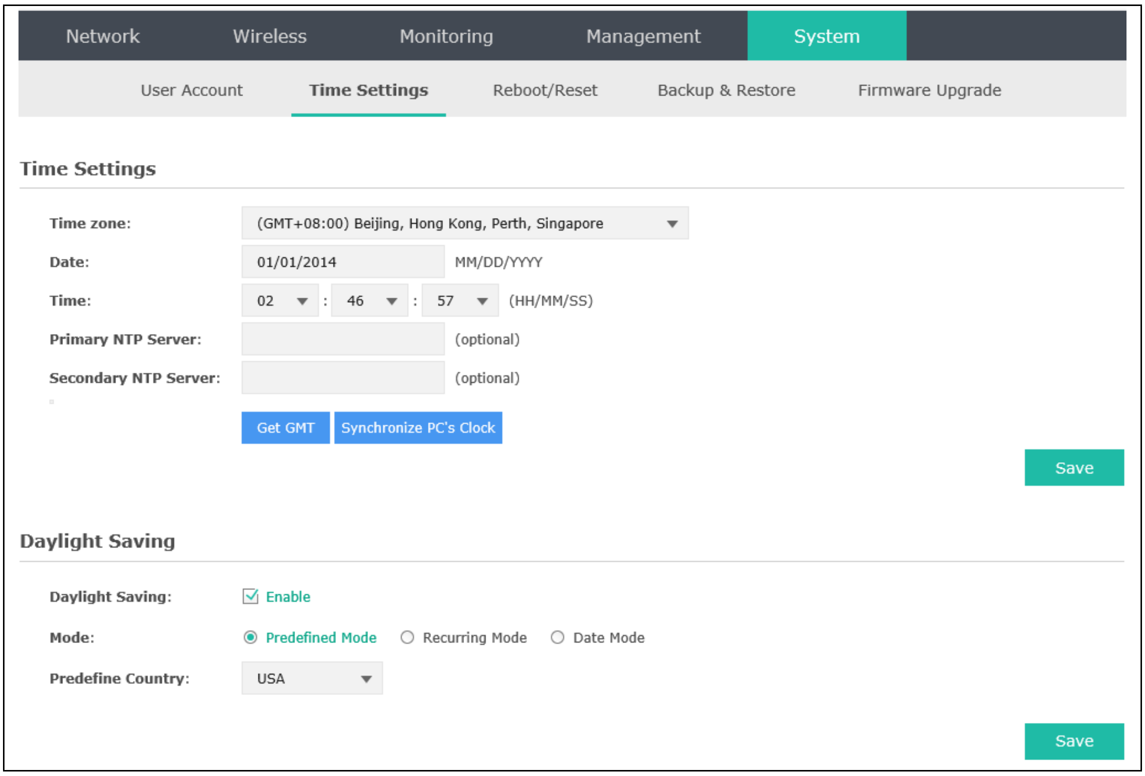
Figure 7-61 User Account Page

Old User Name/Password:	Enter the present user name and password of the admin account to get the permission of modification.
New User Name/Password:	Enter a new user name and password for the admin account. Both values are case-sensitive, up to 64 characters and with no space.
Confirm New Password:	Enter the new password again.

7.5.2 Time Settings

System time represents the device system's notion of the passing of time. System time is the standard time for Scheduler and other time-based functions. You can manually set the system time, configure the system to acquire its time settings from a preconfigured NTP server or synchronize the system time with the PC's clock.

The device supports DST (daylight saving time).



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 01/01/2014 MM/DD/YYYY

Time: 02 : 46 : 57 (HH/MM/SS)

Primary NTP Server: (optional)

Secondary NTP Server: (optional)

Daylight Saving

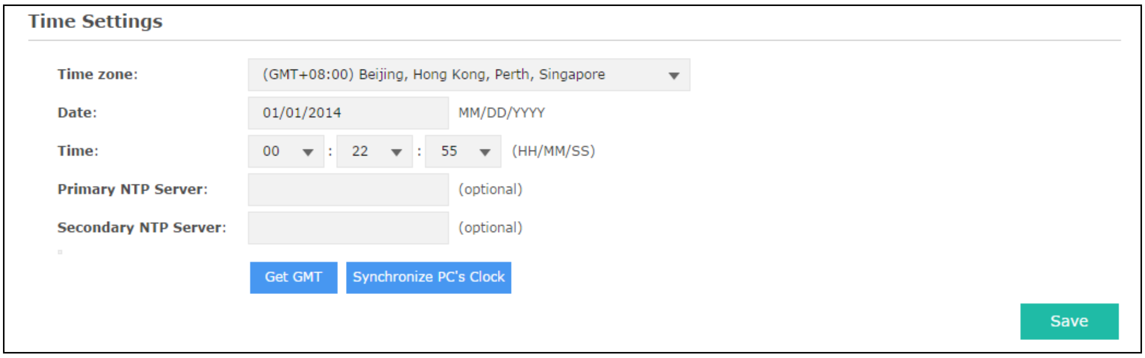
Daylight Saving: ☑ Enable

Mode: ● Predefined Mode ○ Recurring Mode ○ Date Mode

Predefine Country: USA

Figure 7-62 Time Settings

7.5.2.1 Time Settings



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 01/01/2014 MM/DD/YYYY

Time: 00 : 22 : 55 (HH/MM/SS)

Primary NTP Server: (optional)

Secondary NTP Server: (optional)

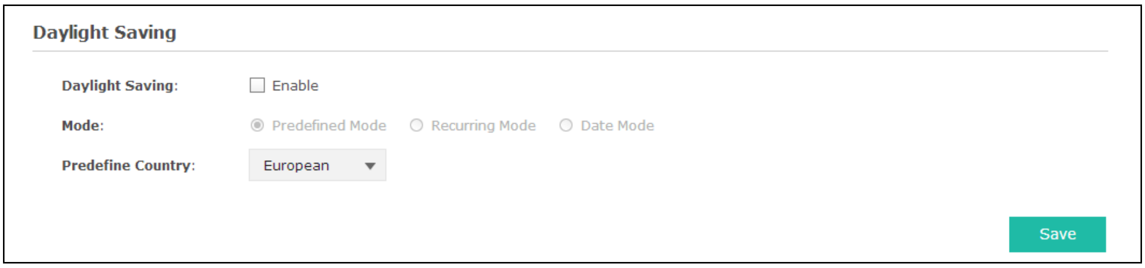
Figure 7-63 Time Settings

Get GMT	Click the button and the device will obtain GMT time from NTP server. IP address of the NTP server has to be filled in.
Synchronize PC's Clock	Click the button, your PC's time will be obtained as the device's system time.
Time zone:	Select your local time zone from the drop-down list.
Date:	Set the current date, in format MM/DD/YYYY. For example, for November 25, 2014, enter 11/25/2014 in the field.

Time: Specify the device's time. Select the number from the drop-down list in time format HH/MM/SS.

Primary/Secondary NTP Server: If you've selected **Get GMT** from an NTP server, please input the primary NTP sever address and an alternative NTP server address.

7.5.2.2 Daylight Saving



Daylight Saving

Daylight Saving: □ Enable

Mode: ● Predefined Mode ○ Recurring Mode ○ Date Mode

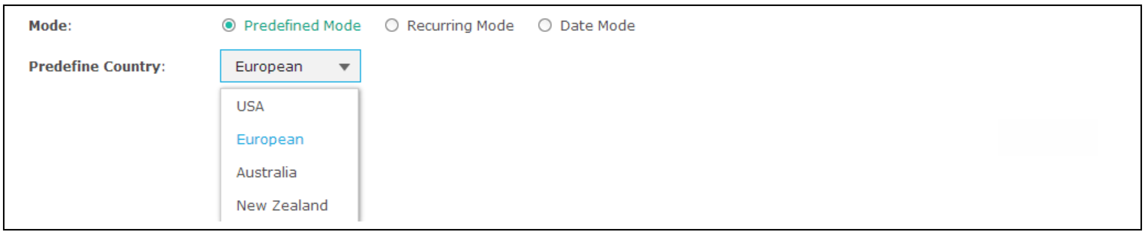
Predefine Country: European

Figure 7-64 Daylight Saving

Daylight Saving: Enable or disable the DST. DST is disabled by default.

Mode: Options include Predefined Mode, Recurring Mode and Date Mode. Please refer to the following content for more information.

Predefined Mode



Mode: ● Predefined Mode ○ Recurring Mode ○ Date Mode

Predefine Country: European

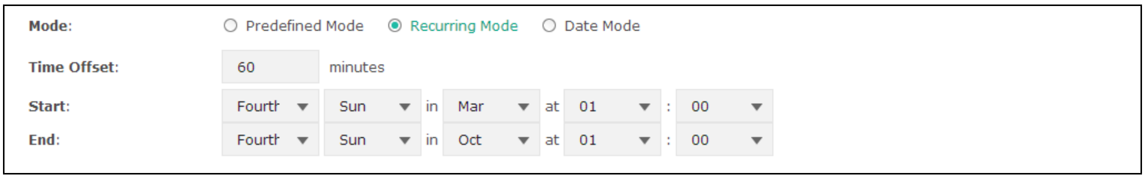
Figure 7-65 Predefined Mode

Mode: Select **Predefined Mode**.

Predefine Country: Select a predefined DST configuration. Europe is the predefined country by default.

- **USA**: Second Sunday in March, 02:00 ~ First Sunday in November, 02:00
- **European**: Last Sunday in March, 01:00 ~ Last Sunday in October, 01:00
- **Australia**: First Sunday in October, 02:00 ~ First Sunday in April, 03:00
- **New Zealand**: Last Sunday in September, 02:00 ~ First Sunday in April, 03:00

- ## Recurring Mode



Mode: ○ Predefined Mode ● Recurring Mode ○ Date Mode

Time Offset: 60 minutes

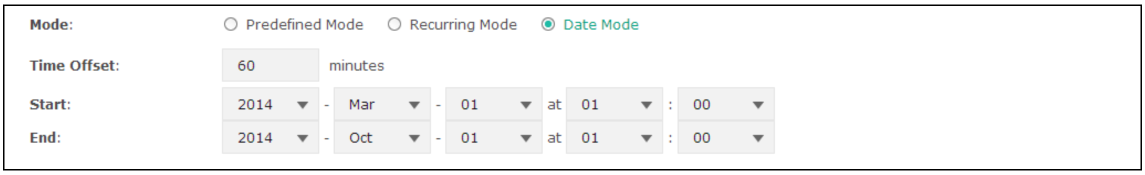
Start: Fourth Sun in Mar at 01 : 00

End: Fourth Sun in Oct at 01 : 00

Figure 7-66 Recurring Mode

Mode:	Select **Recurring Mode**. The configuration is recurring in use.
Time Offset:	Specify the time adding in minutes when Daylight Saving Time comes.
Start/End:	Select starting time and ending time of Daylight Saving Time.

- ## Date Mode



Mode: ○ Predefined Mode ○ Recurring Mode ● Date Mode

Time Offset: 60 minutes

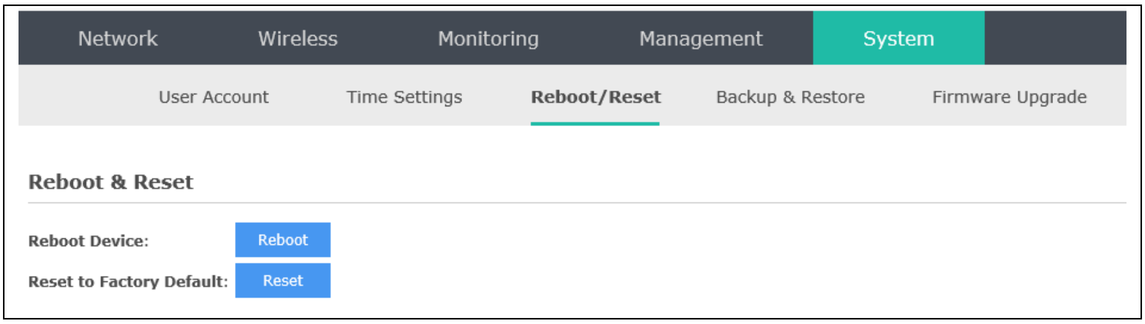
Start: 2014 - Mar - 01 at 01 : 00

End: 2014 - Oct - 01 at 01 : 00

Figure 7-67 Date Mode

Mode:	Select **Date Mode**.
Time Offset:	Specify the time adding in minutes when Daylight Saving Time comes.
Start/End:	Select starting time and ending time of Daylight Saving Time.

7.5.3 Reboot/Reset



Reboot & Reset

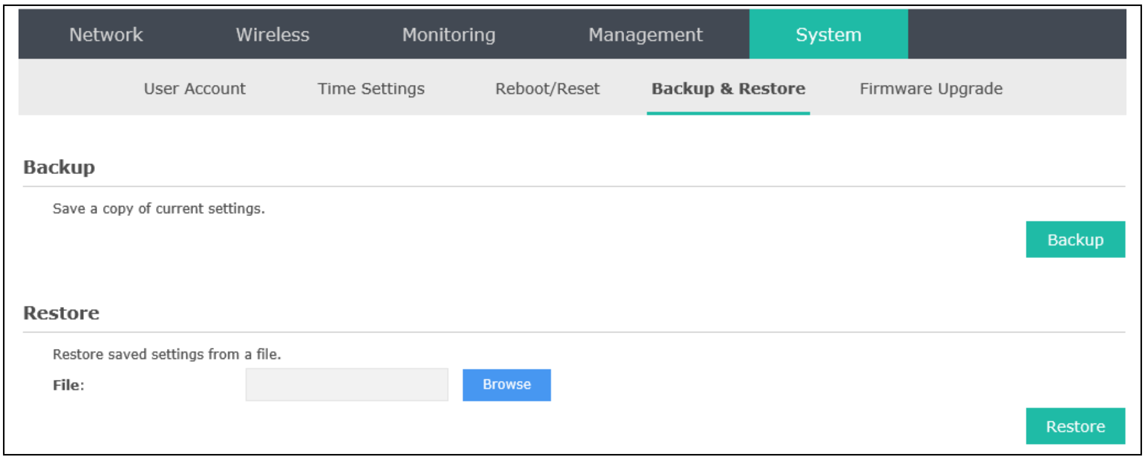
Reboot Device: Reboot

Reset to Factory Default: Reset

Figure 7-68 Reboot & Reset

Click **Reboot** to restart the device. Click **Reset** to restore the device to factory default settings.

7.5.4 Backup & Restore



Backup

Save a copy of current settings.

Restore

Restore saved settings from a file.

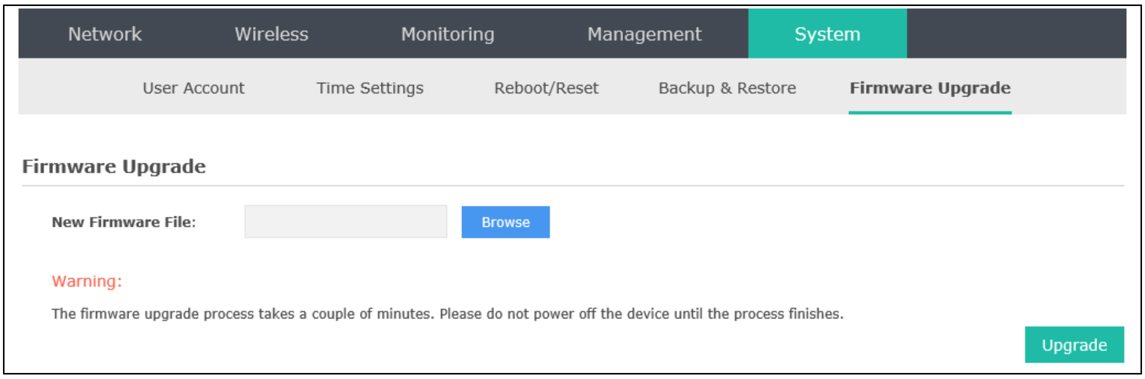
File:

Figure 7-69 Backup & Restore

You can save the current configuration of the EAP as a backup file and restore the configuration via a backup file. Back up the settings before you upgrade the device or upload a new configuration file can prevent it from being lost.

Restore function helps you to restore the device to previous settings by uploading a backup file.

7.5.5 Firmware Upgrade



Firmware Upgrade

New Firmware File:

Warning:

The firmware upgrade process takes a couple of minutes. Please do not power off the device until the process finishes.

Figure 7-70 Firmware Upgrade

Please log in http://www.tp-link.com/en/support/download/ to download the latest system file. Click **Browse** to choose the firmware file. Click **Upgrade** to upgrade the devices.

NOTE:

3. Please select the proper software version that matches your hardware to upgrade.

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

5. After upgrading, the device will reboot automatically.