

Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values are from 0 to 15.
Minimum Contention Window	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value cannot be higher than the value of Maximum Contention Window.
Maximum Contention Window	The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. This value must be higher than the value of Minimum Contention Window.
TXOP Limit	The TXOP Limit is a station EDCA parameter and only applies to traffic flowing from the client station to the EAP. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME (Wireless Multimedia Extensions) client station has the right to initiate transmissions onto the wireless medium (WM) towards the EAP. The valid values are multiples of 32 between 0 and 8192.

5. Choose whether to enable the following two options according to your need.

No Acknowledgement: ☐ Enable

Unscheduled Automatic Power Save Delivery: ☒ Enable

The following table detailedly explains these options:

No Acknowledgment	With this option enabled, the EAP would not acknowledge frames with QosNoAck. No Acknowledgment is recommended if VoIP phones access the network through the EAP.
Unscheduled Automatic Power Save Delivery	As a power management method, it can greatly improve the energy-saving capacity of clients.

6. Click **Save**.

2.8 Configure Rogue AP Detection

A Rogue AP is an access point that is installed on a secure network without explicit authorization from the network administrator. With Rogue AP Detection, the EAP can scan all channels to detect the nearby APs and display the detected APs in the Detected Rogue AP list. If the specific AP is known as safe, you can move it to the Trusted APs list. Also, you can backup and import the Trusted AP list as needed.

Note:

The Rogue AP Detection feature is only used for collecting information of the nearby wireless network and does not impact the detected APs, no matter what operations you have executed in this feature.

To configure Rogue AP Detection, go to the **Wireless > Rogue AP Detection** page.

The screenshot shows the TP-Link web interface. The top navigation bar includes the TP-Link logo and a user profile icon. Below it, a dark blue menu bar has tabs for Status, Wireless (highlighted with a red box), Management, and System. Under the Wireless tab, a sub-menu bar contains links for Wireless Settings, Portal, VLAN, MAC Filtering, Scheduler, Band Steering, QoS, and Rogue AP Detection (highlighted with a red box). The main content area is titled 'Settings' and contains a 'Rogue AP Detection' section with an 'Enable' checkbox and a 'Save' button. Below this is the 'Detected Rogue AP List' section, which includes a 'Scan' button and a table with columns: MAC, SSID, Band, Channel, Security, Beacon Interval, Signal, and Action. The table is currently empty. The next section is 'Trusted AP List', which also contains an empty table with columns: MAC, SSID, Band, Channel, Security, and Action. The final section is 'Download/Backup Trusted AP List', which has radio buttons for 'Download (PC to AP)' (selected) and 'Backup (AP to PC)', a 'Source File Name' field with a 'Browse' button, radio buttons for 'Replace' (selected) and 'Merge', and a 'Save' button.

tp-link

Status **Wireless** Management System

Wireless Settings Portal VLAN MAC Filtering Scheduler Band Steering QoS **Rogue AP Detection**

Settings

Rogue AP Detection: ☐ Enable

Save

Detected Rogue AP List

Scan

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

Trusted AP List

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

Download/Backup Trusted AP List

Save Action: ☒ Download (PC to AP) ☐ Backup (AP to PC)

Source File Name: Browse

File Management: ☒ Replace ☐ Merge

Save

Detect Rogue APs and Move the Rogue APs to the Trusted AP List

Follow the steps below to detect the nearby APs and move the trusted ones to the Trusted AP list.

1. In the **Settings** section, check the box to enable **Rogue AP Detection**. Click **Save**.

Settings

Rogue AP Detection: ☒ **Enable**

Save

2. In the **Detected Rogue AP List** section, click **Scan**.
3. Wait for a few seconds without any operation. After detection is finished, the detected APs will be displayed in the list.

Detected Rogue AP List							
MAC	SSID	Band	Channel	Security	Beacon Interval	Signal	Action
00:0A:EB:13:09:17	C7v3_5G	5.0	36	ON	100		Known
00:0A:EB:13:09:18	C7v3	2.4	11	ON	100		Known
00:0A:EB:13:7A:FD	TP-Link_7B00_5G_1	5.0	36	ON	100		Known
00:0A:EB:13:7A:FE	TP-Link_7B00_5G_2	5.0	36	ON	100		Known
00:0A:EB:13:7A:FF	TP-Link_7B00	2.4	1	ON	100		Known
00:0A:EB:13:7B:01	RvR5	5.0	48	OFF	100		Known
00:1D:0F:E3:33:B1	Camera	2.4	4	ON	100		Known
00:20:02:16:38:22	TP-LINK_2.4G_3822	2.4	1	ON	100		Known
02:71:CC:4C:16:B8	DIRECT-na-BRAVIA	2.4	11	ON	100		Known
06:18:D6:C1:92:23	qwer	2.4	6	OFF	100		Known
12345...8							

The following table introduces the displayed information of the APs:

MAC	Displays the MAC address of the AP.
SSID	Displays the SSID of the AP.
Band	Displays the frequency band the AP is working on.
Channel	Displays the channel the AP is using.
Security	Displays whether the security mode is enabled on the AP.

Beacon Interval	Displays the Beacon Interval value of the EAP. Beacon frames are sent periodically by the AP to announce to the stations the presence of a wireless network. Beacon Interval determines the time interval of the beacon frames sent by the AP device.
Signal	Displays the signal strength of the AP.

- To move the specific AP to the Trusted AP list, click **Known** in the **Action** column. For example, we move the first two APs in the above Detected Rogue AP list to the Trusted AP list.
- View the trusted APs in the **Trusted AP List** section. To move the specific AP back to the Rogue AP list, you can click **Unknown** in the **Action** column.

Trusted AP List					
MAC	SSID	Band	Channel	Security	Action
00:0A:EB:13:7A:FD	TP-Link_7B00_5G_1	5.0	36	ON	Unknown
00:0A:EB:13:7A:FE	TP-Link_7B00_5G_2	5.0	36	ON	Unknown

Manage the Trusted AP List

You can download the trusted AP list from your local host to the EAP or backup the current Trusted AP list to your local host.

• Download the Trusted AP List From the Host

You can import a trusted AP list which records the MAC addresses of the trusted APs. The AP whose MAC address is in the list will not be detected as a rogue AP.

Download/Backup Trusted AP List

Save Action:
☒ Download (PC to AP)
☐ Backup (AP to PC)

Source File Name:

File Management:
☒ Replace
☐ Merge

Follow the steps below to import a trusted AP list to the EAP:

- Acquire the trusted AP list. There are two ways:
 - Backup the list from a EAP. For details, refer to [Backup the Trusted AP List to the Host](#).

- Manually create a trusted AP list. Create a txt. file, input the MAC addresses of the trusted APs in the format XX:XX:XX:XX:XX:XX and use the Space key to separate each MAC address. Save the file as a **cfg** file.
2. On this page, check the box to choose **Download (PC to AP)**.
 3. Click **Browse** and select the trusted AP list from your local host.
 4. Select the file management mode. Two modes are available: **Replace** and **Merge**. Replace means that the current trusted AP list will be replaced by the one you import. Merge means that the APs in the imported list will be added to the current list with the original APs remained.
 5. Click **Save** to import the trusted AP list.

- **Backup the Trusted AP List to the Host**

You can backup the current trusted AP list and save the backup file to the local host.

Download/Backup Trusted AP List

Save Action: ☐ Download (PC to AP) ☒ Backup (AP to PC)

Save

Follow the steps below to backup the current trusted AP list:

1. On this page, check the box to choose **Backup (AP to PC)**.
2. Click **Save** and the current trusted AP list will be downloaded to your local host as a **cfg** file.

3

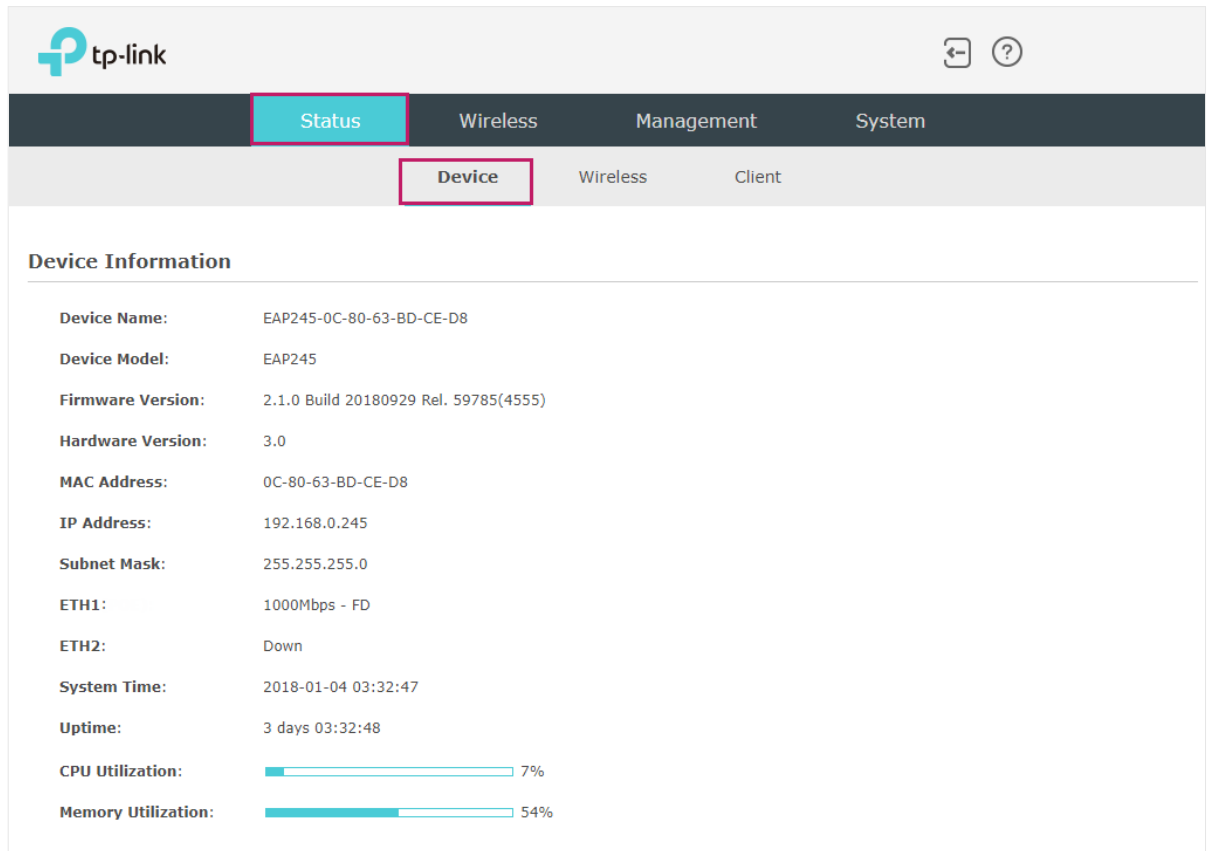
Monitor the Network

This chapter introduces how to monitor the running status and statistics of the wireless network, including:

- *3.1 Monitor the EAP*
- *3.2 Monitor the Wireless Parameters*
- *3.3 Monitor the Clients*

3.1 Monitor the EAP

To monitor the EAP information, go to the **Status > Device** page.



The screenshot shows the TP-Link web interface. The top navigation bar has 'Status' highlighted. Below it, the 'Device' sub-tab is selected. The 'Device Information' section displays the following details:

Device Name:	EAP245-0C-80-63-BD-CE-D8
Device Model:	EAP245
Firmware Version:	2.1.0 Build 20180929 Rel. 59785(4555)
Hardware Version:	3.0
MAC Address:	0C-80-63-BD-CE-D8
IP Address:	192.168.0.245
Subnet Mask:	255.255.255.0
ETH1:	1000Mbps - FD
ETH2:	Down
System Time:	2018-01-04 03:32:47
Uptime:	3 days 03:32:48
CPU Utilization:	7%
Memory Utilization:	54%

The following device information is displayed:

Device Name	Displays the name of the EAP. The name consists of the product model followed with the MAC address of the EAP by default.
Device Model	Displays the product model of the EAP.
Firmware Version	Displays the current firmware version the EAP. To update the firmware, you can refer to 5.6 Update the Firmware .
Hardware Version	Displays the hardware version the EAP.
MAC Address	Displays the MAC address of the EAP.
IP Address	Displays the IP address of the EAP.
Subnet Mask	Displays the subnet mask of the EAP.
System Time	Displays the current system time. To configure the system time, you can refer to 5.3 Configure the System Time .
Uptime	Displays how long the EAP has been working since it starts up.

CPU Utilization	Displays the CPU occupancy. If this value is too high, the EAP may work abnormally.
Memory Utilization	Displays the memory occupancy.

3.2 Monitor the Wireless Parameters

You can view the wireless parameters of the EAP, including SSID lists, radio settings, radio traffic and LAN traffic.

Tips:

To change the wireless parameters, you can refer to [2.1 Configure the Wireless Parameters](#).

To monitor the wireless parameters, go to the **Status > Wireless** page.



StatusWirelessManagementSystem

DeviceWirelessClient

SSID List

 Refresh

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	SSID-1	0	2.4GHz	WPA-PSK	Disable	Disable	Disable	922k	82k
2	SSID-2	0	5GHz	None	Disable	Disable	Disable	12k	2k

Radio Settings

2.4GHz5GHz

2.4GHz Wireless Radio: Enable

Channel Frequency: 6 / 2437MHz

Channel Width: 20/40MHz

IEEE802.11 Mode: b/g/n mixed

Max TX Rate: 300.0Mbps

Tx Power: 20dBm

Radio Traffic

2.4GHz5GHz

Rx Packets: 66730494

Rx Bytes: 16998586607

Rx Dropped Packets: 0

Rx Errors: 0

Tx Packets: 7099989

Tx Bytes: 1610535114

Tx Dropped Packets: 0

Tx Errors: 65

LAN Traffic

Rx Packets: 455929

Rx Bytes: 259238847

Rx Dropped Packets: 0

Rx Errors: 0

Tx Packets: 169208

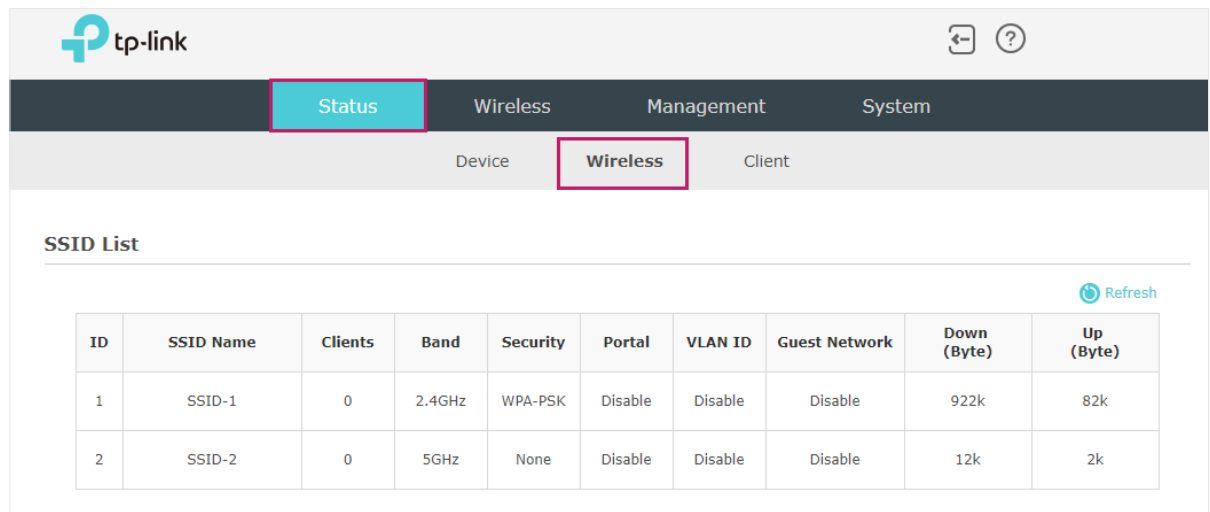
Tx Bytes: 167366153

Tx Dropped Packets: 0

Tx Errors: 0

Monitor the SSIDs

You can monitor the SSID information of the EAP.



The screenshot shows the TP-Link web interface. At the top, there's a navigation bar with 'Status' highlighted. Below it, a sub-navigation bar has 'Wireless' highlighted. The main content area is titled 'SSID List' and contains a table with 10 columns: ID, SSID Name, Clients, Band, Security, Portal, VLAN ID, Guest Network, Down (Byte), and Up (Byte). There are two rows of data. A 'Refresh' button is located at the top right of the table.

ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Byte)	Up (Byte)
1	SSID-1	0	2.4GHz	WPA-PSK	Disable	Disable	Disable	922k	82k
2	SSID-2	0	5GHz	None	Disable	Disable	Disable	12k	2k

The following table introduces the displayed information of the SSID:

SSID Name	Displays the SSID name.
Clients	Displays the number of clients currently connected to the SSID.
Band	Displays the frequency band the SSID is currently using.
Security	Displays the security mode of the SSID.
Portal	Displays whether portal function is enabled on the SSID.
VLAN ID	Displays the VLAN ID of the SSID.
Guest Network	Display guest network is enabled on the SSID.
Down (Byte)	Displays the total download traffic since the SSID starts working.
Up (Byte)	Displays the total upload traffic since the SSID starts working.

Monitor the Radio Settings

You can monitor the radio settings of the EAP. For a dual-band EAP, there are two bands: 2.4GHz and 5GHz. You can click to select a band to view. The following figure posted in the introduction takes 2.4GHz as an example.

Radio Settings

2.4GHz5GHz

2.4GHz Wireless Radio:

Enable

Channel Frequency:

6 / 2437MHz

Channel Width:

20/40MHz

IEEE802.11 Mode:

b/g/n mixed

Max TX Rate:

300.0Mbps

Tx Power:

20dBm

The following table introduces the displayed information of the EAP.

2.4GHz/5GHz Wireless Radio	Displays whether wireless function is enabled on the radio band.
Channel Frequency	Displays the channel and frequency which are currently used by the EAP.
Channel Width	Displays the channel width which is currently used by the EAP.
IEEE802.11 Mode	Displays the IEEE802.11 protocol currently used by the EAP.
Max TX Rate	Displays the maximum physical rate of the EAP.
Tx Power	Displays the transmit power of the EAP.

Monitor Radio Traffic

You can monitor the radio traffic of the EAP. For a dual-band EAP, there are two bands: 2.4GHz and 5GHz. You can click to select a band to view. The following figure posted in the introduction takes 2.4GHz as an example.

Radio Traffic

2.4GHz5GHz

Rx Packets:

82874437

Rx Bytes:

20906526476

Rx Dropped Packets:

0

Rx Errors:

0

Tx Packets:

8800930

Tx Bytes:

1990845129

Tx Dropped Packets:

0

Tx Errors:

65

The following traffic information of the radio is displayed:

Rx Packets	Displays the total number of the received packets on the 2.4GHz/5GHz band since the EAP starts up.
Tx Packets	Displays the total number of the sent packets on the 2.4GHz/5GHz band since the EAP starts up.
Rx Bytes	Displays the total received traffic on the 2.4GHz/5GHz band since the EAP starts up.
Tx Bytes	Displays the total sent traffic on the 2.4GHz/5GHz band since the EAP starts up.
Rx Dropped Packets	Displays the total number of the dropped packets which are received on the 2.4GHz/5GHz band since the EAP starts up.
Tx Dropped Packets	Displays the total number of the dropped packets which are sent on the 2.4GHz/5GHz band since the EAP starts up.
Rx Errors	Displays the total number of error packets which are received on the 2.4GHz/5GHz band since the EAP starts up.
Tx Errors	Displays the total number of error packets which are sent on the 2.4GHz/5GHz band since the EAP starts up.

Monitor LAN Traffic

You can view the LAN traffic of EAP.

LAN Traffic			
Rx Packets:	559223	Tx Packets:	206607
Rx Bytes:	320073875	Tx Bytes:	204207153
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

The following traffic information of the LAN is displayed:

Rx Packets	Displays the total number of received packets in the LAN since the EAP starts up.
Tx Packets	Displays the total number of sent packets in the LAN since the EAP starts up.
Rx Bytes	Displays the total received traffic in the LAN since the EAP starts up.
Tx Bytes	Displays the total sent traffic in the LAN since the EAP starts up.

Rx Dropped Packets	Displays the total number of the dropped packets which are received by the EAP since it starts up.
Tx Dropped Packets	Displays the total number of the dropped packets which are sent by the EAP since it starts up.
Rx Errors	Displays the total number of the received error packets since the EAP starts up.
Tx Errors	Displays the total number of the sent error packets since the EAP starts up.

3.3 Monitor the Clients

You can monitor the information of the clients connected to the EAP.

To monitor the client information, go to the **Status > Client** page.

The screenshot shows the TP-Link web interface. At the top, there's a navigation bar with 'Status' highlighted. Below it, a sub-navigation bar shows 'Device', 'Wireless', and 'Client' (highlighted). The main content area is divided into two sections: 'Client List' and 'Block Client List'.

Client List

Buttons: User (selected), Guest

Refresh button

ID	Hostname	IP Address	MAC Address	Band	SSID	Active Time	Up (Byte)	Down (Byte)	RSSI (dBm)	Rate (Mbps)	Action
1	iPhone	192.168.1.100	D0-A6-37-83-DA-99	5GHz	SSID-2	0 days 00:01:24	39k	20k	-83	263.0	

Block Client List

Refresh button

ID	Hostname	MAC Address	Up (Byte)	Down (Byte)	Action
1	android-6532c20e9aa005cc	1C-77-F6-91-C7-B8	3k	1k	

View Client Information

There are two types of clients: users and portal authenticated guests. Users are the clients that connect to the SSID with portal authentication disabled. Guests are the clients that connect to the SSID with portal authentication enabled.

Click the **User** button to select the client types to view the information of the EAP. The following figure posted in the introduction takes user as an example.

The screenshot shows the TP-Link web interface with the 'Client List' section. The 'User' button is selected, and the 'Guest' button is unselected. The table displays client information for a single user.

Client List

Buttons: User (selected), Guest

Refresh button

ID	Hostname	IP Address	MAC Address	Band	SSID	Active Time	Up (Byte)	Down (Byte)	RSSI (dBm)	Rate (Mbps)	Action
1	iPhone	192.168.1.100	D0-A6-37-83-DA-99	5GHz	SSID-2	0 days 00:00:07	4k	1k	-80	175.0	

The following client information is displayed:

Hostname	Displays the hostname of the user.
IP Address	Displays the IP address of the user.

MAC Address	Displays the MAC address of the user.
Band	Displays the frequency band the user is working on.
SSID	Displays the SSID the user is connecting to.
Active Time	Displays how long the user has been connected to the SSID.
Up (Byte)	Displays the user's total uploaded traffic to the EAP since the last connection.
Down (Byte)	Displays the user's total downloaded traffic from the EAP since the last connection.
RSSI (dBm)	Displays the RSSI(Received Signal Strength Indication) of the user.
Rate (Mbps)	Displays the wireless transmission rate of the user.

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



Click the icon to configure the rate limit of the client to balance bandwidth usage. Enter the download limit and upload limit and click **OK**.

You can limit the download and upload rate for each clients by which connect to specific SSIDs when configuring SSIDs, refer to [2.1.1 Configure SSIDs](#) to get more details.

Note that the download and upload rate will be limited to the smaller value if you set the limit value both in SSID and client configuration.

Rate Limit:

☒ Enable
 ?

Download Limit:

Kbps

(1-10240000)

Upload Limit:

Kbps

(1-10240000)

OK



Click the icon to block the access of the client to the network.

View Block Client Information

You can view the information of the clients that have been blocked and resume the client's access.

Block Client List					
					 Refresh
ID	Hostname	MAC Address	Up (Byte)	Down (Byte)	Action
1	android-6532c20e9aa005cc	1C-77-F6-91-C7-B8	3k	1k	

The following information of the blocked client is displayed:

Hostname	Displays the hostname of the user.
MAC Address	Displays the MAC address of the user.
Up (Byte)	Displays the user's total uploaded traffic to the EAP since the last connection.
Down (Byte)	Displays the user's total downloaded traffic from the EAP since the last connection.
Action	You can click the  to resume the client's access to the internet.

4

Manage the EAP

The EAP provides powerful functions of device management and maintenance. This chapter introduces how to manage the EAP, including:

- *4.1 Manage the IP Address of the EAP*
- *4.2 Manage System Logs*
- *4.3 Configure Web Server*
- *4.4 Configure Management Access*
- *4.5 Configure LED*
- *4.6 Configure Wi-Fi Control (Only for Certain Devices)*
- *4.7 Configure PoE Out (Only for Certain Devices)*
- *4.8 Configure SSH*
- *4.9 Configure SNMP*

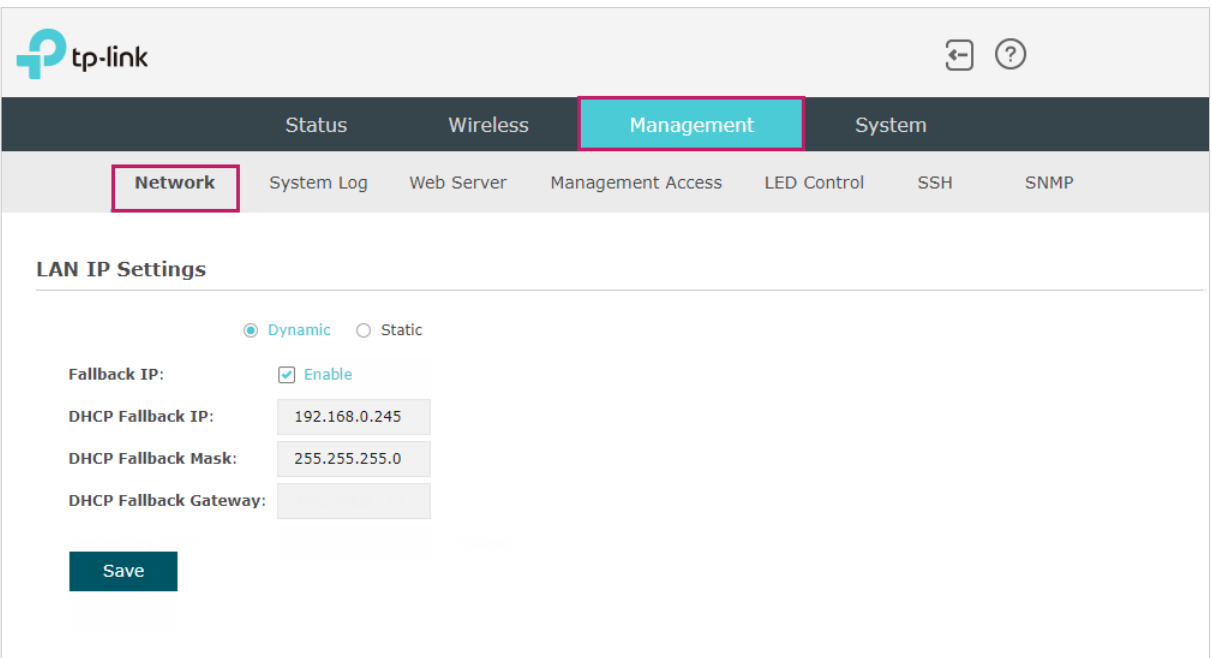
4.1 Manage the IP Address of the EAP

The IP address of the EAP can be a dynamic IP address assigned by the DHCP server or a static IP address manually specified by yourself. By default, the EAP gets a dynamic IP address from the DHCP server. You can also specify a static IP address according to your needs.

Tips:

For detailed introduction about how to find the dynamic IP address of the EAP, refer to [Using Web Browser on Your PC and Connecting to the Ethernet](#).

To configure the IP address of the EAP, go to the **Management > Network** page.



The screenshot shows the TP-Link web interface. At the top, the 'tp-link' logo is on the left, and navigation icons are on the right. Below the logo, there are four main tabs: 'Status', 'Wireless', 'Management' (highlighted with a red box), and 'System'. Under the 'Management' tab, there are several sub-tabs: 'Network' (highlighted with a red box), 'System Log', 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The 'Network' sub-tab is active, showing the 'LAN IP Settings' section. In this section, there are two radio buttons: 'Dynamic' (selected) and 'Static'. Below these, there is a 'Fallback IP' section with a checkbox labeled 'Enable' (checked). Underneath, there are three input fields: 'DHCP Fallback IP' with the value '192.168.0.245', 'DHCP Fallback Mask' with the value '255.255.255.0', and 'DHCP Fallback Gateway' which is empty. At the bottom of the section is a 'Save' button.

Follow the steps below to configure the IP address of the EAP:

1. Choose your desired IP address mode: **Dynamic** or **Static**.
2. Configure the related parameters according to your selection.

- **Dynamic**

If you choose Dynamic as the IP address mode, make sure that there is a reachable DHCP server on your network and the DHCP sever is properly configured to assign IP address and the other network parameters to the EAP.

Dynamic Static

Fallback IP: ☒ Enable

DHCP Fallback IP: 192.168.0.245

DHCP Fallback Mask: 255.255.255.0

DHCP Fallback Gateway:

For network stability, you can also configure the fallback IP parameters for the EAP:

Fallback IP	With the fallback IP configured, if the EAP fails to get an IP address from a DHCP server within 10 seconds, the fallback IP will work as the IP address of the EAP. After that, however, the EAP will keep trying to obtain an IP address from the DHCP server until it succeeds.
DHCP Fallback IP	Specify a fallback IP address for the EAP. Make sure that this IP address is not being used by any other device in the same LAN. The default DHCP fallback IP is 192.168.0.254.
DHCP Fallback IP MASK	Specify the network mask of the fallback IP. The default DHCP fallback IP mask is 255.255.255.0.
DHCP Fallback Gateway	Specify the network gateway.

- **Static**

If you choose Static as the IP address mode, you need to manually specify an IP address and the related network parameters for the EAP. Make sure that the specified IP address is not being used by any other device in the same LAN.

Dynamic Static

IP Address: 192.168.0.245

IP Mask: 255.255.255.0

Gateway: 0.0.0.0

Primary DNS: 192.168.0.1

Secondary DNS: 0.0.0.0 (Optional)

Configure the IP address and network parameters as the following table shows:

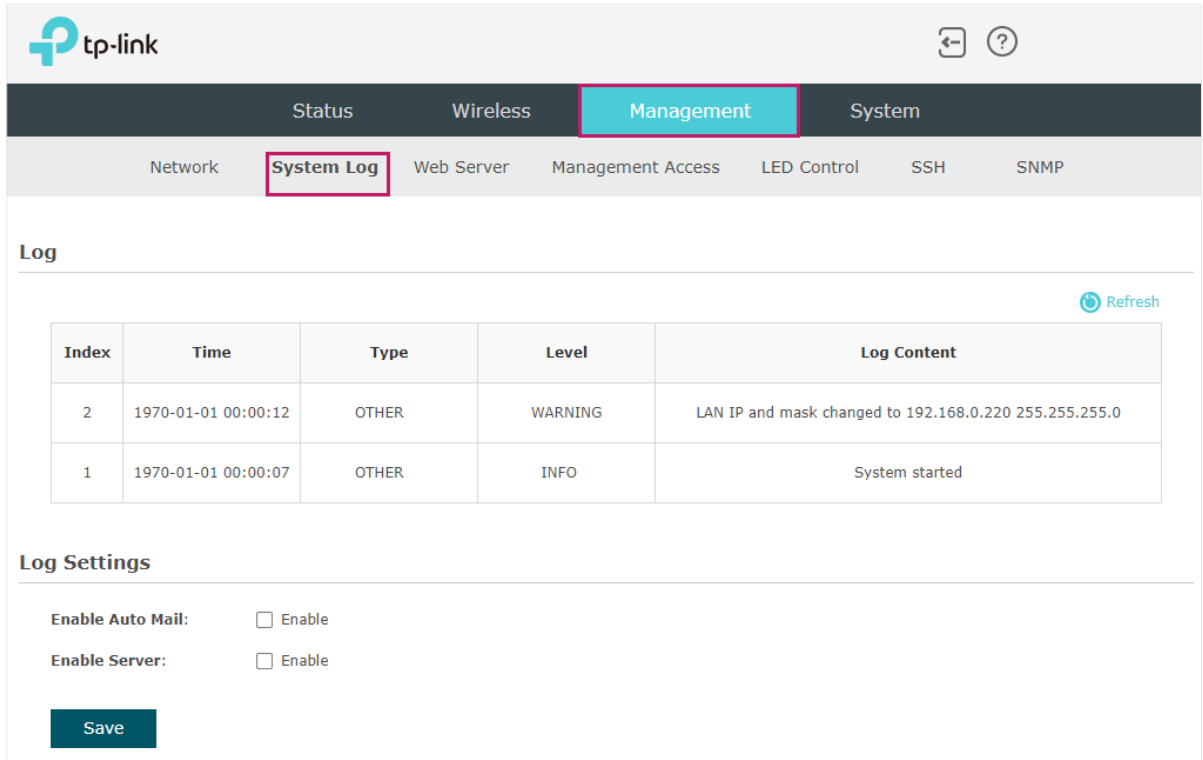
IP Address	Specify a static IP address for the EAP.
IP Mask	Specify the network mask.
Gateway	Specify the network gateway.
Primary DNS	Specify the primary DNS server.
Secondary DNS	Specify the secondary DNS server. (Optional)

3. Click **Save**.

4.2 Manage System Logs

System logs record 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.

To manage system logs, go to the **Management > System Log** page.



The screenshot shows the TP-Link web interface. The top navigation bar includes the TP-Link logo and a help icon. Below it, a dark blue bar contains 'Status', 'Wireless', 'Management' (highlighted with a red box), and 'System'. Under 'Management', a sub-bar shows 'Network', 'System Log' (highlighted with a red box), 'Web Server', 'Management Access', 'LED Control', 'SSH', and 'SNMP'. The 'Log' section features a table with the following data:

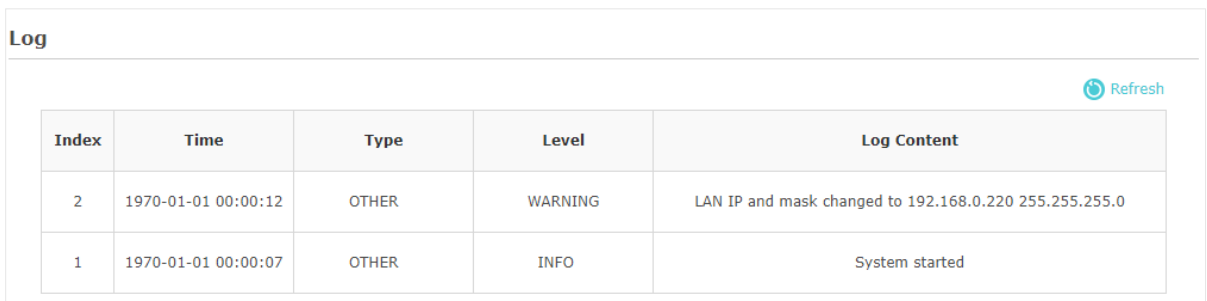
Index	Time	Type	Level	Log Content
2	1970-01-01 00:00:12	OTHER	WARNING	LAN IP and mask changed to 192.168.0.220 255.255.255.0
1	1970-01-01 00:00:07	OTHER	INFO	System started

Below the table is the 'Log Settings' section, which includes two checkboxes: 'Enable Auto Mail' and 'Enable Server', both currently unchecked. A 'Save' button is located at the bottom of this section.

On this page, you can view the system logs and configure the way of receiving system logs.

View System Logs

In the **Log** section, you can click  **Refresh** to refresh the logs and view them in the table.



The screenshot shows the 'Log' section of the TP-Link web interface. It features a table with the following data:

Index	Time	Type	Level	Log Content
2	1970-01-01 00:00:12	OTHER	WARNING	LAN IP and mask changed to 192.168.0.220 255.255.255.0
1	1970-01-01 00:00:07	OTHER	INFO	System started

A 'Refresh' button is located in the top right corner of the table area.

Configure the Way of Receiving Logs

In the **Log Settings** section, you can configure the ways of receiving system logs.

Log Settings

Enable Auto Mail:

☐ Enable

Enable Server:

☐ Enable

Save

Follow the steps below to configure this feature:

1. Check the corresponding box to enable one or more ways of receiving system logs, and configure the related parameters. Two ways are available: [Auto Mail](#) and [Server](#).

■ Auto Mail

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

Note:

SSL encryption is not currently supported.

Enable Auto Mail:

☒ Enable

From:

To:

SMTP Server:

Enable Authentication:

☐ Enable

Time:

☒ Fixed Time ☐ Period

Fixed Time:

00 ▾

:

00 ▾

(HH:MM)

The following table introduces how to configure these parameters:

From	Enter the sender's E-mail address.
To	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the sender's SMTP server. Note: At present, the domain name of SMTP server is not supported in this field.
Enable Authentication	If the sender's mailbox is configured with You can check the box to enable mail server authentication. Enter the sender's username and password.

Time Mode	Select Time Mode: Fixed Time or Period Time . Fixed Time means that the system logs will be sent at the specific time every day. Period Time means that the system logs will be sent at the specific time interval.
Fixed Time	If you select Fixed Time , specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday.
Period Time	If you select Period Time , specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours.

■ Server

If Server is configured, system logs will be sent to the specified system log server, and you can use the syslog software to view the logs on the server.

Enable this feature and enter the IP address and port of the system log server.

Enable Server:	☒ Enable
System Log Server IP:	0.0.0.0
System Log Server Port:	514
More Client Detail Log:	☐ Enable

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

2. Click **Save**.

4.3 Configure Web Server

With the web server, you can log in to the management web page of the EAP. You can configure the web server parameters of the EAP according to your needs.

To configure Web Server, go to the **Management > Web Server** page.

The screenshot shows the TP-Link Omada web interface. The top navigation bar has tabs for Status, Wireless, Management (selected), and System. Under the Management tab, there are sub-tabs: Network, System Log, Web Server (selected), Management Access, LED Control, SSH, and SNMP. The Web Server configuration page displays the following settings:

Secure Server Port:	443
Server Port:	80
Session Timeout:	15 minutes
Layer-3 Accessibility:	☐ Enable

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

Save

Follow the steps below to configure Web Server:

1. Refer to the following table to configure the parameters:

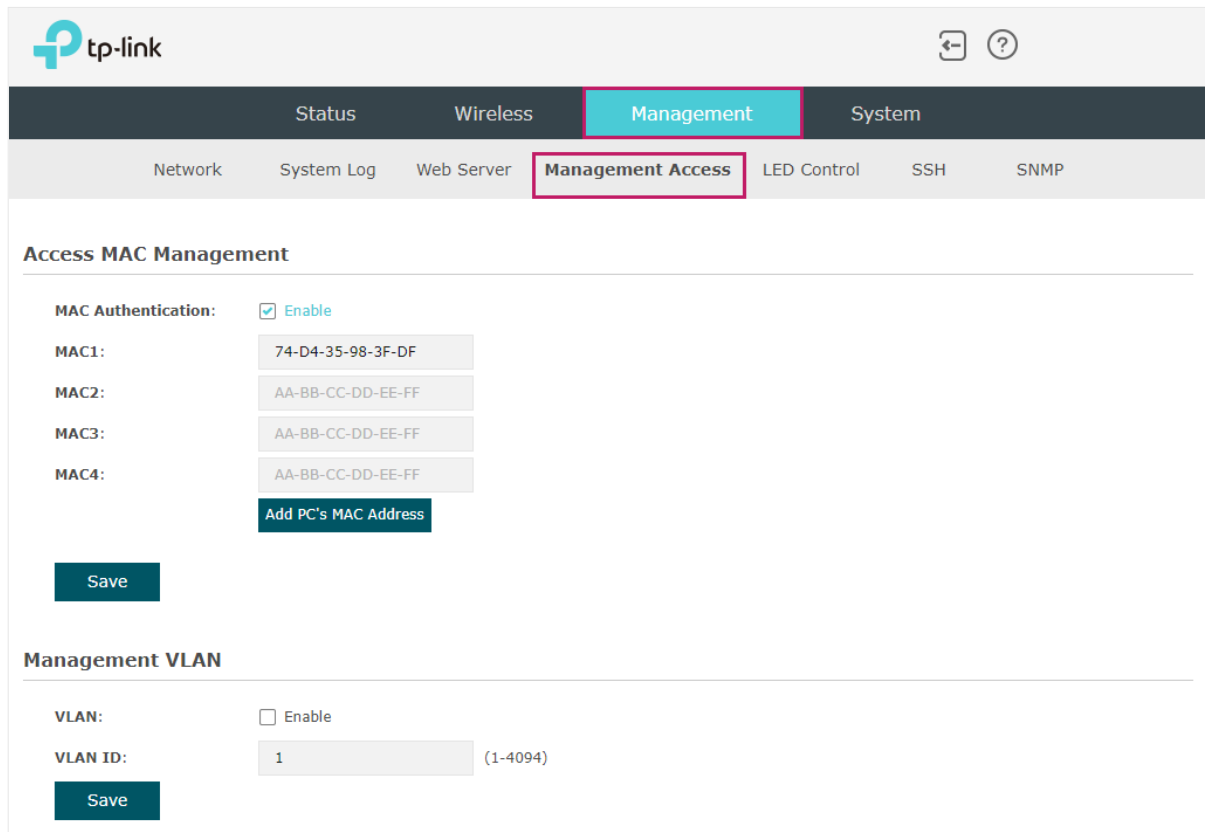
Secure Server Port	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
Server Port	Designate a server port for web server in HTTP mode. By default the port is 80.
Session Timeout	Set the session timeout. If you do nothing with the web page within the timeout, the system will log out automatically. You can log in again if you want to go back to web page.
Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access Omada managed devices via the management web page. With this feature disabled, only the devices in the same subnet can access Omada managed devices via the management web page.

2. Click **Save**.

4.4 Configure Management Access

By default, all hosts in the LAN can log in to the management web page of the EAP with the correct username and password. To control the hosts' access to the web page of the EAP, you can specify the MAC addresses and management VLAN of the hosts that are allowed to access the web page.

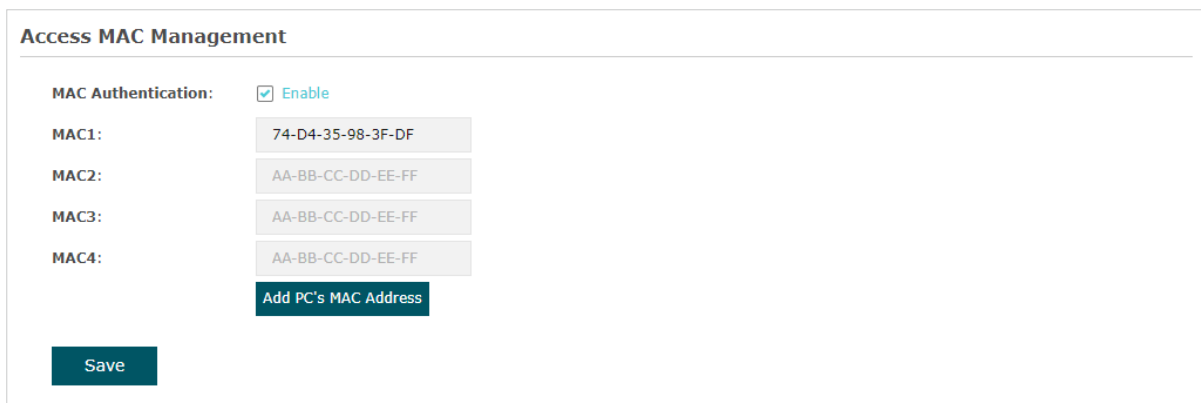
To configure Management Access, go to the **Management > Management Access** page.



The screenshot shows the TP-Link web interface. The top navigation bar includes 'Status', 'Wireless', 'Management' (highlighted in blue), and 'System'. Below this, a sub-navigation bar shows 'Network', 'System Log', 'Web Server', 'Management Access' (highlighted with a red box), 'LED Control', 'SSH', and 'SNMP'. The main content area is titled 'Access MAC Management'. It contains two sections: 'MAC Authentication' and 'Management VLAN'. In the 'MAC Authentication' section, the 'Enable' checkbox is checked. Below it are four input fields for MAC addresses (MAC1, MAC2, MAC3, MAC4), each containing a placeholder address (74-D4-35-98-3F-DF, AA-BB-CC-DD-EE-FF, AA-BB-CC-DD-EE-FF, AA-BB-CC-DD-EE-FF). There is a button labeled 'Add PC's MAC Address' and a 'Save' button. The 'Management VLAN' section has an 'Enable' checkbox which is unchecked. Below it is a 'VLAN ID' input field with the value '1' and a range '(1-4094)', followed by a 'Save' button.

Configure Access MAC Management

Only the hosts with the specific MAC addresses are allowed to access the web page, and other hosts without MAC addresses specified are not allowed to access the web page.



This screenshot shows the 'Access MAC Management' configuration page, which is identical to the one above. It displays the 'MAC Authentication' section with 'Enable' checked and four MAC address input fields. The 'Management VLAN' section shows 'Enable' unchecked and a 'VLAN ID' of 1. Both sections have 'Save' buttons and an 'Add PC's MAC Address' button.

Follow the steps below to configure Management Access on this page:

1. Check the box to enable **MAC Authentication**.
2. Specify one or more MAC addresses in the **MAC1/MAC2/MAC3/MAC4** fields. Up to four MAC addresses can be added.
3. Click **Save**.

Tips:

- You can click **Add PC's MAC Address** to quickly add the MAC address of your current logged-in host, .
- Verify the MAC addresses carefully. Once the settings are saved, only the hosts in the MAC address list can access the web page of the EAP.
- If you cannot log in to the web page after saving the wrong configuration, you can reset the EAP to the factory defaults and use the default username and password (both admin) to log in.

Configure Management VLAN

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

Management VLAN

VLAN:

☐ Enable

VLAN ID:

(1-4094)

Save

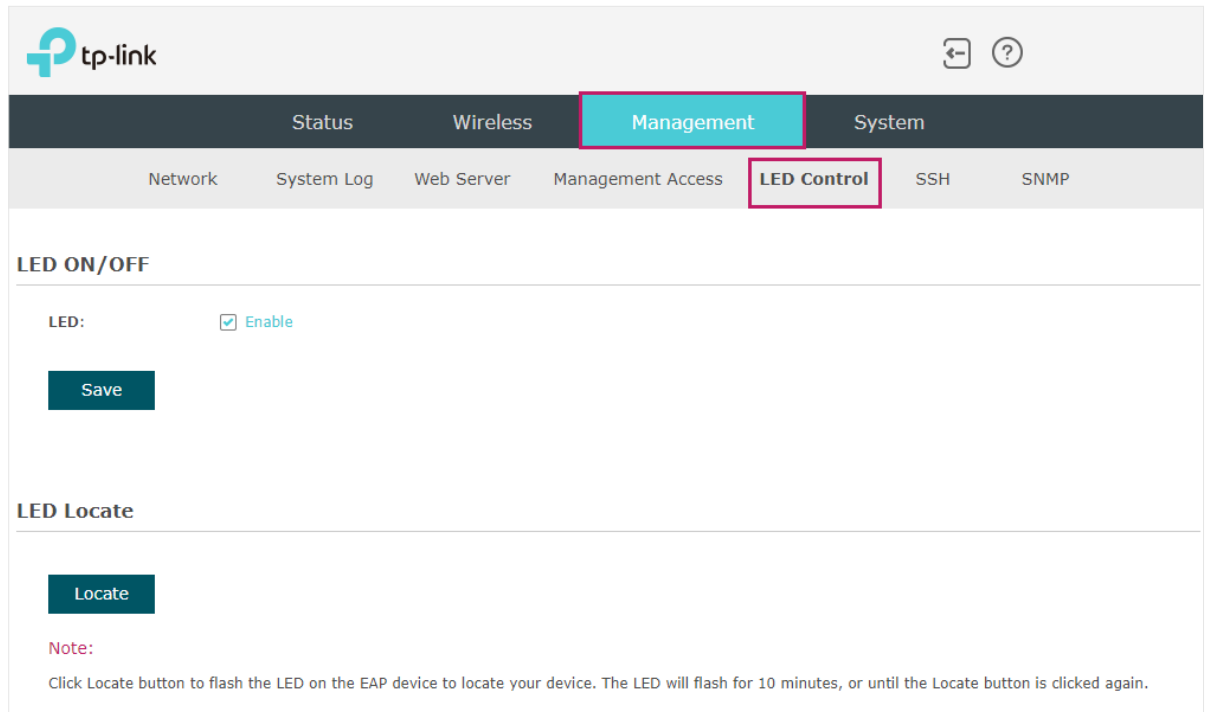
Follow the steps below to configure Management VLAN on this page:

1. Check the box to enable **Management VLAN**.
2. Specify the VLAN ID of the management VLAN. Only the hosts in the Management VLAN can log in to the EAP via the Ethernet port.
3. Click **Save**.

4.5 Configure LED

You can turn on or off the LED light of the EAP and flash the LED to locate your device.

To configure LED, go to the **Management > LED Control** page.



tp-link

Status Wireless **Management** System

Network System Log Web Server Management Access **LED Control** SSH SNMP

LED ON/OFF

LED: ☒ Enable

Save

LED Locate

Locate

Note:
Click Locate button to flash the LED on the EAP device to locate your device. The LED will flash for 10 minutes, or until the Locate button is clicked again.

Check the box to turn on or turn off the LED light of the EAP, and click **Save**. To flash the LED, click **Locate**. Then the LED will flash for 10 minutes or until the locate button is clicked again.

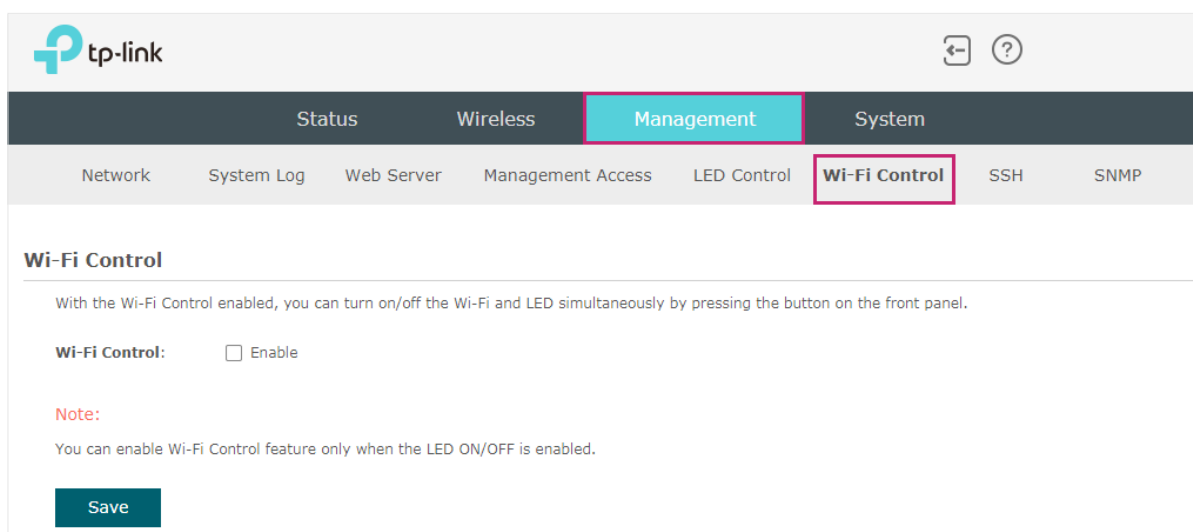
4.6 Configure Wi-Fi Control (Only for Certain Devices)

Note:

Wi-Fi Control is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If Wi-Fi Control is available, there is **Management > Wi-Fi Control** in the menu structure.

Certain devices have an LED/Wi-Fi button on the front panel. With Wi-Fi Control enabled, you can press the button to turn on or off both of the Wi-Fi and LED at the same time.

To configure Wi-Fi Control, go to the **Management > Wi-Fi Control** page.



The screenshot shows the TP-Link web interface. At the top, there is a navigation bar with the TP-Link logo on the left and a help icon on the right. Below this is a main menu with tabs: Status, Wireless, Management (highlighted in blue), and System. Under the Management tab, there is a sub-menu with links: Network, System Log, Web Server, Management Access, LED Control, Wi-Fi Control (highlighted with a red box), SSH, and SNMP. The main content area is titled "Wi-Fi Control". It contains a paragraph: "With the Wi-Fi Control enabled, you can turn on/off the Wi-Fi and LED simultaneously by pressing the button on the front panel." Below this is a label "Wi-Fi Control:" followed by an unchecked checkbox and the text "Enable". A red "Note:" section follows, stating: "You can enable Wi-Fi Control feature only when the LED ON/OFF is enabled." At the bottom of the form is a blue "Save" button.

Check the box to enable Wi-Fi Control and click **Save**.

Note:

You can enable Wi-Fi Control only when the option **LED ON/OFF** is enabled.

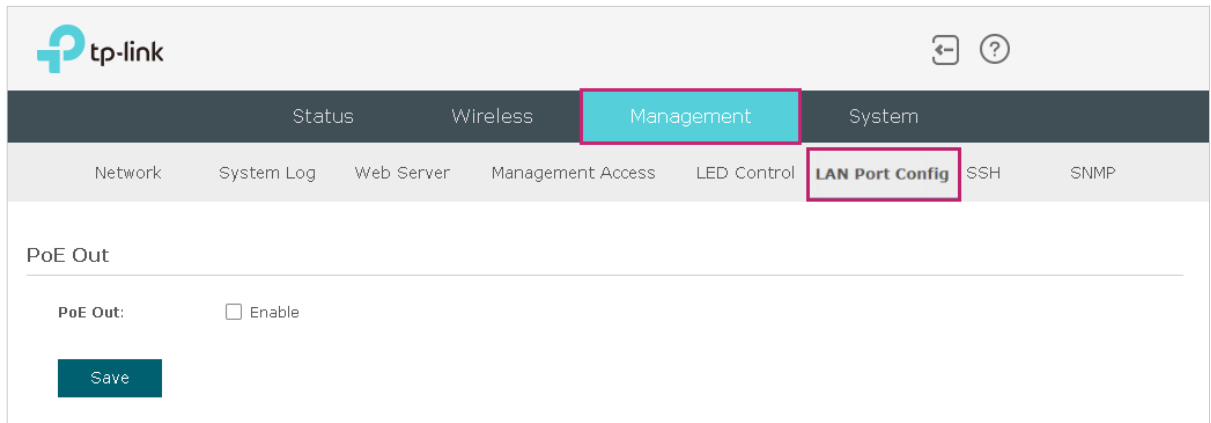
4.7 Configure PoE Out (Only for Certain Devices)

Note:

PoE Out is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. If PoE Out is available, there is **Management > LAN Port Config** in the menu structure.

Certain devices have a PoE OUT port that can transmit data and supply power to the client simultaneously. You can also disable PoE Out to make the port transmit data only.

To configure PoE Out, go to the **Management > LAN Port Config** page.



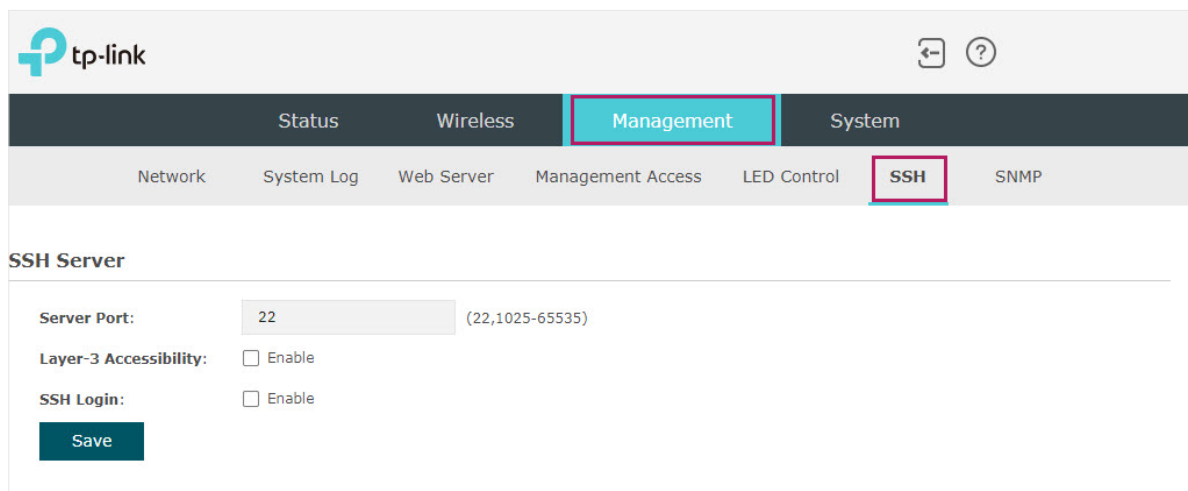
The screenshot shows the TP-Link web interface. At the top left is the TP-Link logo. To the right are icons for a home page and a help page. Below the logo is a navigation bar with four main tabs: Status, Wireless, Management, and System. The Management tab is highlighted with a red border. Below this bar is a secondary navigation bar with several sub-items: Network, System Log, Web Server, Management Access, LED Control, LAN Port Config (highlighted with a red border), SSH, and SNMP. The main content area is titled 'PoE Out'. It contains a label 'PoE Out:' followed by an unchecked checkbox and the text 'Enable'. At the bottom of this section is a red 'Save' button.

Check the box to enable PoE Out and click **Save**.

4.8 Configure SSH

If you want to remotely log in to the EAP via SSH, you can deploy an SSH server on your network and configure the SSH feature on the EAP.

To configure SSH, go to the **Management > SSH** page.



The screenshot shows the TP-Link Omada web interface. The top navigation bar includes 'Status', 'Wireless', 'Management' (highlighted), and 'System'. Below this, a secondary navigation bar shows 'Network', 'System Log', 'Web Server', 'Management Access', 'LED Control', 'SSH' (highlighted), and 'SNMP'. The main content area is titled 'SSH Server' and contains the following configuration options:

- Server Port:** A text input field containing '22' and a tooltip showing '(22,1025-65535)'.
- Layer-3 Accessibility:** A checkbox labeled 'Enable' which is currently unchecked.
- SSH Login:** A checkbox labeled 'Enable' which is currently unchecked.
- A **Save** button at the bottom.

Follow the steps below to configure SSH on this page:

1. Refer to the following table to configure the parameters:

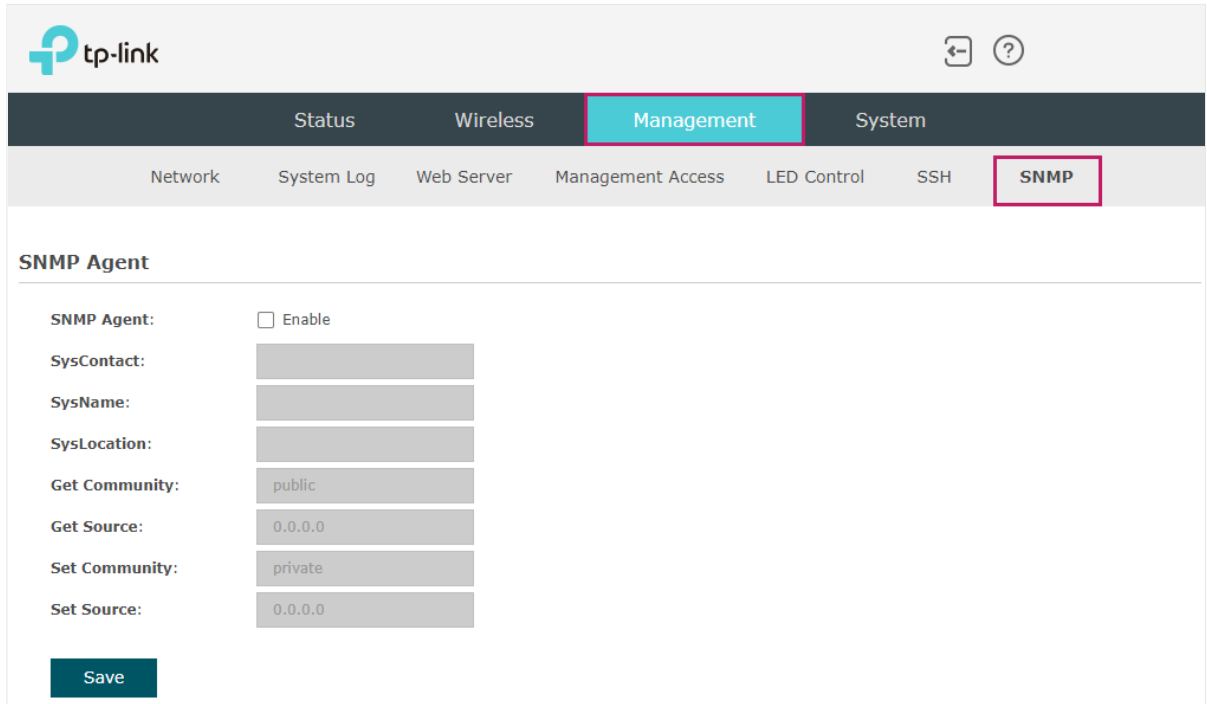
Server Port	Designate a server port for SSH. By default the port is 22.
Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access Omada managed devices via SSH. With this feature disabled, only the devices in the same subnet can access Omada managed devices via SSH.
SSH Login	Enable or disable SSH Login globally.

2. Click **Save**.

4.9 Configure SNMP

The EAP can be configured as an SNMP agent and work together with the SNMP manager. Once the EAP has become an SNMP agent, it is able to receive and process request messages from the SNMP manager. At present, the EAP supports SNMP v1 and v2c.

To configure the EAP as an SNMP agent, go to the **Management > SNMP** page.



The screenshot shows the TP-Link web interface. The top navigation bar has tabs for Status, Wireless, Management (highlighted), and System. Below this, a secondary navigation bar includes Network, System Log, Web Server, Management Access, LED Control, SSH, and SNMP (highlighted). The main content area is titled 'SNMP Agent' and contains the following configuration options:

- SNMP Agent:** ☐ Enable
- SysContact:** [Text input field]
- SysName:** [Text input field]
- SysLocation:** [Text input field]
- Get Community:** [Text input field with value 'public']
- Get Source:** [Text input field with value '0.0.0.0']
- Set Community:** [Text input field with value 'private']
- Set Source:** [Text input field with value '0.0.0.0']

A 'Save' button is located at the bottom left of the configuration area.

Follow the steps below to complete the configuration on this page:

1. Check the box to enable **SNMP Agent**.
2. Refer to the following table to configure the required parameters:

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) for management systems that can serve as Get Community to read the SNMP information of this device. 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) for management systems that can serve as Set Community to read and write the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read and write the SNMP information of this device.

3. Click **Save**.

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 recommend that modify 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.

5

Configure the System

This chapter introduces how to configure the system of the EAP, including:

- *5.1 Configure the User Account*
- *5.2 Controller Settings*
- *5.3 Configure the System Time*
- *5.4 Reboot and Reset the EAP*
- *5.5 Backup and Restore the Configuration*
- *5.6 Update the Firmware*

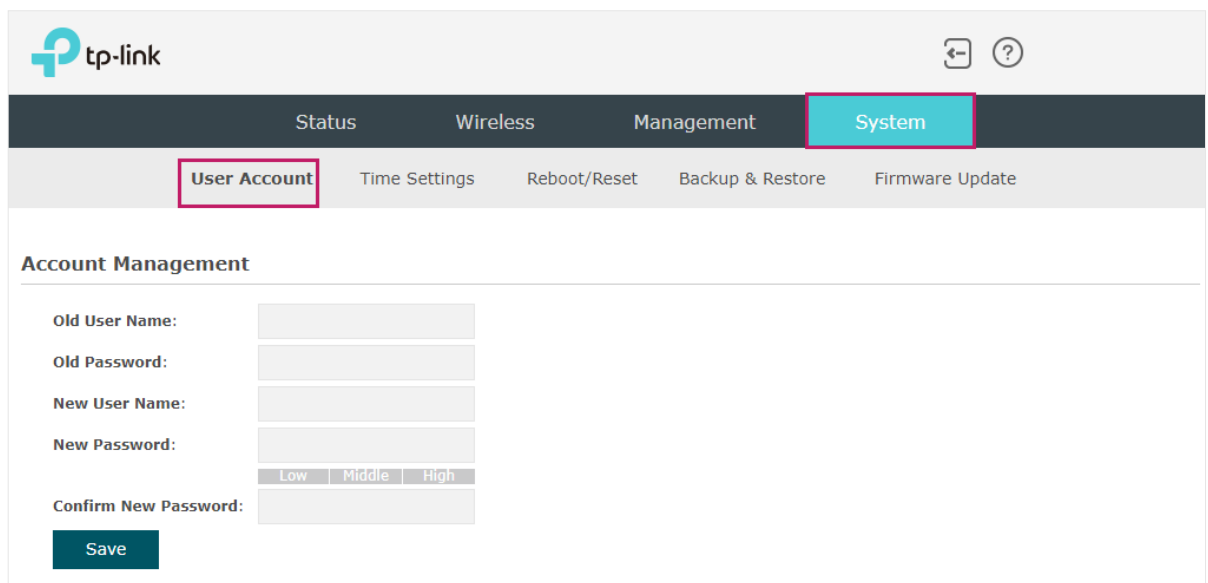
5.1 Configure the User Account

Every EAP has a user account, which is used to log in to the management page of the EAP. When you start the EAP at the first time, the username and password of the user account are both admin. After the first login, the system will require you to set a new username and a new password for the user account. And then you can use the new user account to log in to the EAP. Also, you can change your user account as needed.

Tips:

Please remember your user account well. If you forget it, reset the EAP to the factory defaults and log in with the default user account (username and password are both admin).

To configure the user account, go to **System > User Account** page.



The screenshot shows the TP-Link EAP management interface. At the top, there is a navigation bar with the TP-Link logo and a help icon. Below this is a main menu with tabs: Status, Wireless, Management, and System. The System tab is selected and highlighted in blue. Under the System tab, there is a sub-menu with options: User Account, Time Settings, Reboot/Reset, Backup & Restore, and Firmware Update. The User Account option is highlighted with a red box. The main content area is titled 'Account Management' and contains the following fields:

- Old User Name:
- Old Password:
- New User Name:
- New Password:
- Confirm New Password:

Below the New Password field, there are three radio buttons for password strength: Low, Middle, and High. The Low button is selected. At the bottom of the form is a blue 'Save' button.

Follow the steps below to change your user account on this page:

1. Enter the old username and old password of your user account.
2. Specify a new username and a new password for your user account. The system will automatically detect the strength of your entered password. For security, we recommend that you set a password with high strength.
3. Retype the new password.
4. Click **Save**.

5.2 Controller Settings

To make your controller adopt your EAP, make sure the EAP can be discovered by the controller. Controller Settings enable your EAP to be discovered in either of the following scenarios.

- If you are using Omada Cloud-Based Controller, *Enable Cloud-Based Controller Management*.
- If your EAP and controller are located in the same network, LAN and VLAN, the controller can discover and adopt the EAP without any controller settings. Otherwise, you need to inform the EAP of the controller's URL/IP address, and one possible way is to *Configure Controller Inform URL*.

For details about the whole procedure, refer to the User Guide of Omada SDN Controller. The guide can be found on the download center of our official website: <https://www.tp-link.com/support/download/>

Enable Cloud-Based Controller Management

Go to the **System > Controller Settings** page. In the Cloud- Based Controller Management section, enable Cloud-Based Controller Management and click **Save**. After you add the

EAP to your Omada Cloud-Based Controller, you can check the connection status on this page.





StatusWirelessManagementSystem

User AccountController SettingsTime SettingsReboot/ResetBackup & RestoreFirmware Update

Cloud-Based Controller Management

Connection Status: Disabled

Cloud-Based Controller Management: ☐ Enable

Note:

To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.

You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address:

Note:

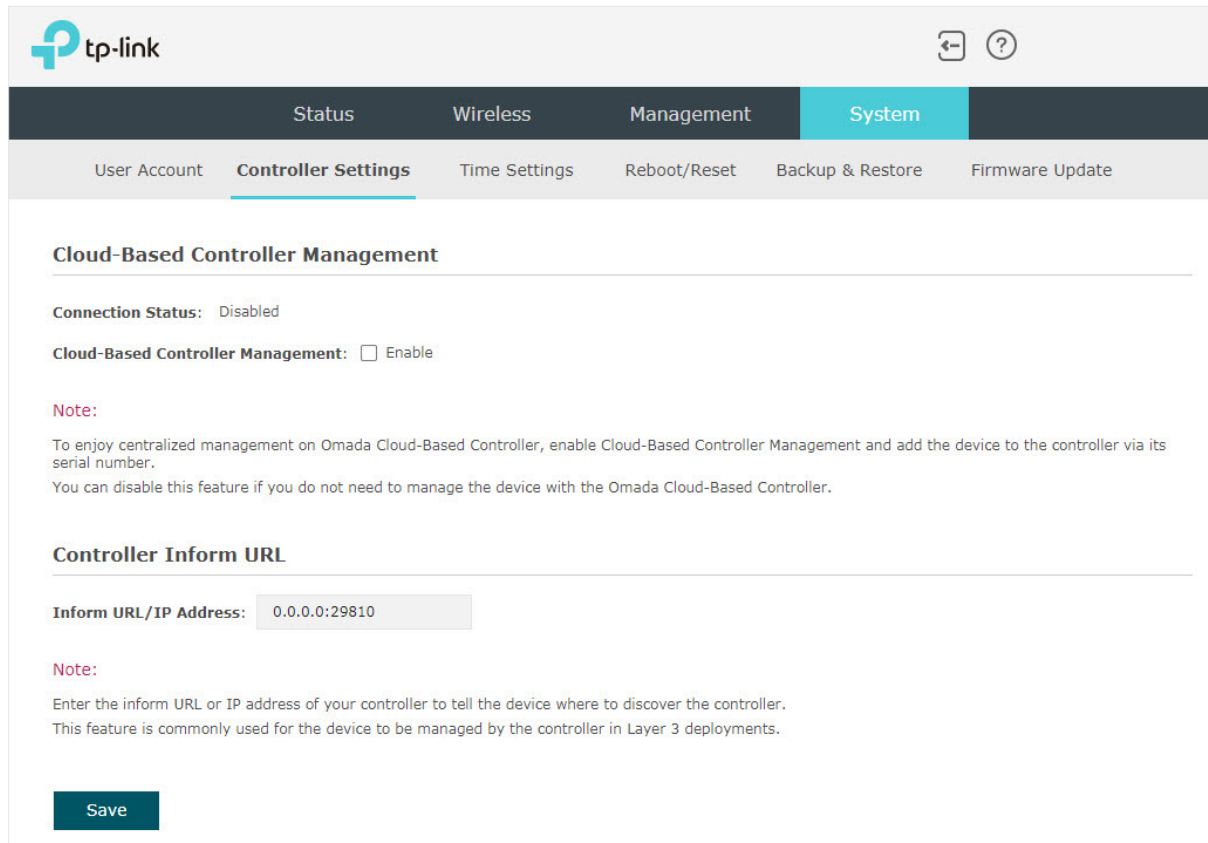
Enter the inform URL or IP address of your controller to tell the device where to discover the controller.

This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

Save

Configure Controller Inform URL

Go to the **System > Controller Settings** page. In the Controller Inform URL section, inform the EAP of the controller's URL/IP address, and click **Save**. Then the EAP make contact with the controller so that the controller can discover the EAP.



The screenshot shows the TP-Link Omada web interface. The top navigation bar includes the TP-Link logo and a help icon. Below it, a dark blue menu bar contains 'Status', 'Wireless', 'Management', and 'System' (which is highlighted). Under the 'System' menu, a sub-menu bar includes 'User Account', 'Controller Settings' (which is highlighted), 'Time Settings', 'Reboot/Reset', 'Backup & Restore', and 'Firmware Update'.

The main content area is titled 'Cloud-Based Controller Management'. It shows 'Connection Status: Disabled' and a toggle for 'Cloud-Based Controller Management' set to 'Disable'. A note explains that enabling this feature allows for centralized management on Omada Cloud-Based Controller.

Below this is the 'Controller Inform URL' section. It contains a label 'Inform URL/IP Address:' followed by a text input field containing '0.0.0.0:29810'. A note below the field states: 'Enter the inform URL or IP address of your controller to tell the device where to discover the controller. This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.'

At the bottom of the section is a dark blue 'Save' button.

5.3 Configure the System Time

System time is the standard time for Scheduler and other time-based functions. The EAP supports the basic system time settings and the Daylight Saving Time (DST) feature.

To configure the system time, go to the **System > Time Settings** page.

Time Settings

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

Date: 06/01/2017 MM/DD/YYYY

Time: 14 : 36 : 21 (HH/MM/SS)

Primary NTP Server: (optional)

Secondary NTP Server: (optional)

Get GMT Synchronize with PC

Save

Daylight Saving

Daylight Saving: ☐ Enable

Mode: ☒ Predefined Mode ☐ Recurring Mode ☐ Date Mode

Predefine Country: European ▼

Save

The following two sections introduce how to configure the basic system time settings and the Daylight Saving Time feature.

Configure the System Time

In the **Time Settings** section, you can configure the system time. There are three methods to set the system time: *Set the System Time Manually*, *Acquire the System Time From an NTP Server*, and *Synchronize the System Time with PC's Clock*.

Time Settings

Time zone:

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

Date:

06/01/2017

MM/DD/YYYY

Time:

14

:

36

:

21

(HH/MM/SS)

Primary NTP Server:

(optional)

Secondary NTP Server:

(optional)

Get GMT

Synchronize with PC

Save

Determine the way of setting the system time and follow the steps below to complete the configurations:

- **Set the System Time Manually**

To set the system time manually, follow the steps below:

1. Configure the following three options on the page: **Time Zone**, **Date** and **Time**.

Time Zone	Select your time zone from the drop-down list. Here GMT means Greenwich Mean Time.
Date	Specify the current date in the format MM/DD/YYYY. MM means month, DD means day and YYYY means year. For example: 06/01/2017.
Time	Specify the current time in the format HH/MM/SS. HH means hour, MM means minute and SS means second. It uses 24-hour system time. For example: 14:36:21.

2. Click **Save**.

Note:

The system time set manually will be lost after the EAP is rebooted.

- **Acquire the System Time From an NTP Server**

To get the system time from an NTP server, follow the steps below:

1. Build an NTP server on your network and make sure that it is reachable by the EAP. Or you can simply find an NTP server on the internet and get its IP address.

Note:

If you use an NTP server on the internet, make sure that the gateway address is set correctly on the EAP. Otherwise, the EAP cannot get the system time from the NTP server successfully. To set the gateway address, refer to [2.1 Configure the Wireless Parameters](#).

2. Specify the NTP server for the EAP. If you have two NTP servers, you can set one of them as the primary NTP server, and the other as the secondary NTP server. Once the primary NTP server is down, the EAP can get the system time from the secondary NTP server.

Primary NTP Server	Enter the IP address of the primary NTP server. Note: If you have only one NTP server on your network, enter the IP address of the NTP server in this field.
Secondary NTP Server	Enter the IP address of the secondary NTP server.

3. Click the button **Get GMT** and the acquired system time will be displayed in the **Date** and **Time** fields.
4. Click **Save**.

- **Synchronize the System Time with PC's Clock**

To synchronize the system time with the clock of your currently logged-in host, follow the steps below:

1. Click the button **Synchronize with PC** and the synchronized system time will be displayed in the **Date** and **Time** fields.
2. Click **Save**.

Note:

The system time synchronized with PC's clock will be lost after the EAP is rebooted.

Configure Daylight Saving Time

Daylight saving time is the practice of advancing clocks during summer months so that evening daylight lasts longer, while sacrificing normal sunrise times. The EAP provides daylight saving time configuration.

Daylight Saving

Daylight Saving:

☐ Enable

Mode:

☒ Predefined Mode ☐ Recurring Mode ☐ Date Mode

Predefine Country:

European ▼

Save

Follow the steps below to configure daylight saving time:

1. Check the box to enable **Daylight Saving**.
2. Select the mode of daylight saving time. Three modes are available: **Predefined Mode**, **Recurring Mode** and **Date Mode**.
3. Configure the related parameters of the selected mode.

■ Predefined Mode

If you select Predefined Mode, choose your region from the drop-down list and the EAP will use the predefined daylight saving time of the selected region.

Mode:

☒ Predefined Mode ☐ Recurring Mode ☐ Date Mode

Predefine Country:

European ▼

There are four regions provided: **USA**, **European**, **Australia** and **New Zealand**. The following table introduces the predefined daylight saving time of each region.

USA	From 2: 00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November.
European	From 1: 00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October.
Australia	From 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April.
New Zealand	From 2: 00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.

■ Recurring Mode

If you select Recurring Mode, manually specify a cycle time range for the daylight saving time of the EAP. This configuration will be used every year.

Mode:	☐ Predefined Mode	☒ Recurring Mode	☐ Date Mode
Time Offset:	60	minutes (1-180)	
Start:	Last ▼	Sun ▼	in Mar ▼ at 01 ▼ : 00 ▼
End:	Last ▼	Sun ▼	in Oct ▼ at 01 ▼ : 00 ▼

The following table introduces how to configure the cycle time range.

Time Offset	Specify the time to set the clock forward by.
Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).

■ Date Mode

If you select Date Mode, manually specify an absolute time range for the daylight saving time of the EAP. This configuration will be used only once.

Mode:	☐ Predefined Mode	☐ Recurring Mode	☒ Date Mode
Time Offset:	60	minutes (1-180)	
Start:	2014 ▼	- Mar ▼	- 01 ▼ at 01 ▼ : 00 ▼
End:	2014 ▼	- Oct ▼	- 01 ▼ at 01 ▼ : 00 ▼

The following table introduces how to configure the absolute time range.

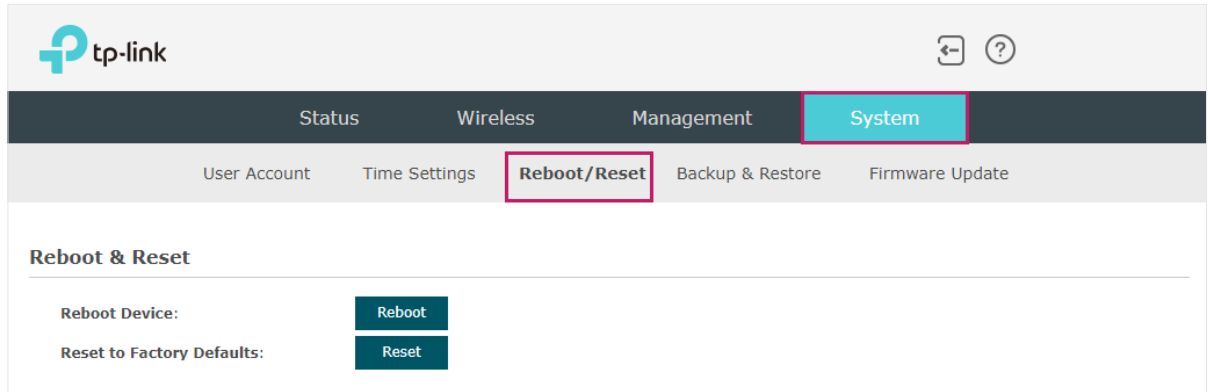
Time Offset	Specify the time to set the clock forward by.
Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).

4. Click **Save**.

5.4 Reboot and Reset the EAP

You can reboot and reset the EAP according to your need.

To reboot and reset the EAP, go to the **System > Reboot&Reset** page.



- To reboot the EAP, click the **Reboot** button , and the EAP will be rebooted automatically. Please wait without any operation.
- To reset the EAP, click the **Reset** button , and the EAP will be reset to the factory defaults automatically. Please wait without any operation.

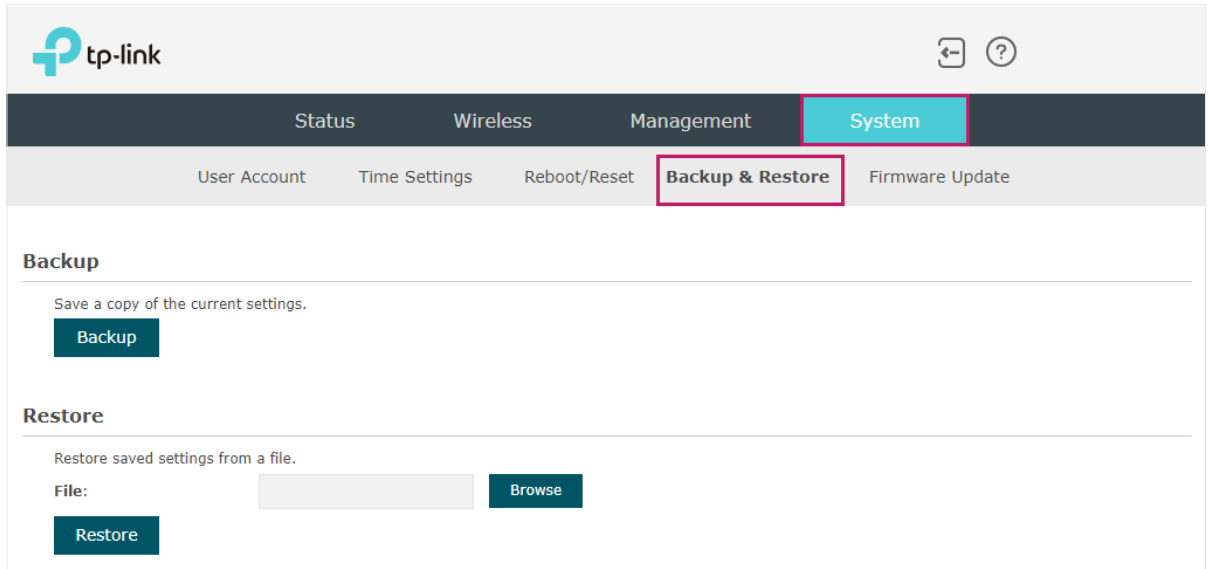
Note:

After reset, all the current configuration of the EAP will be lost. We recommend that you check whether you have any configuration that needs to be backed up before resetting the EAP.

5.5 Backup and Restore the Configuration

You can save the current configuration of the EAP as a backup file and save the file to your host. And if needed, you can use the backup file to restore the configuration. We recommend that you backup the configuration before resetting or upgrading the EAP.

To backup and restore the configuration, go to the **System > Backup&Restore** page.



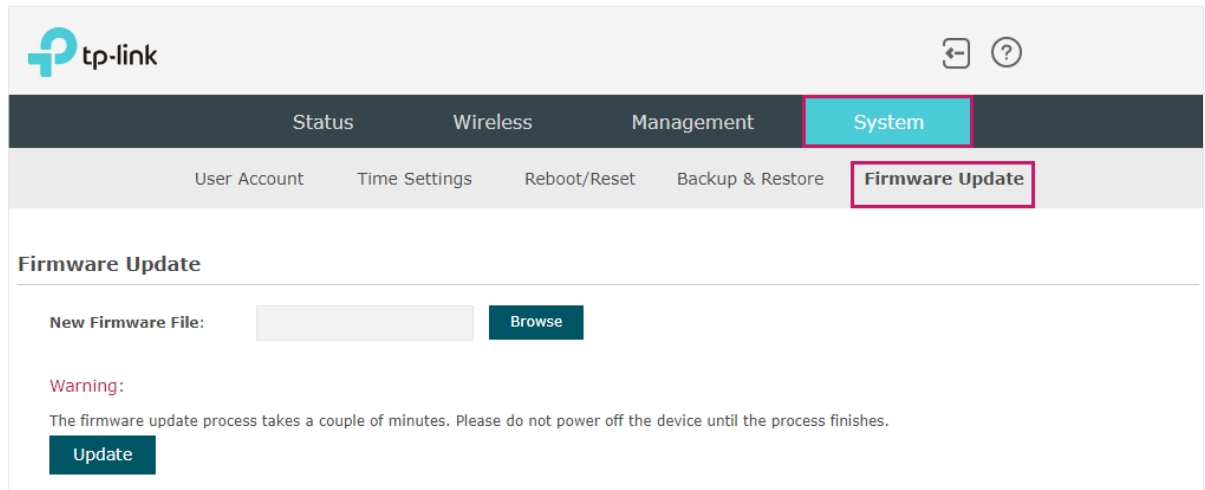
The screenshot shows the TP-Link web interface. At the top, there's a header with the TP-Link logo and navigation icons. Below the header is a dark navigation bar with tabs: Status, Wireless, Management, System (highlighted in red), and an additional tab. Under the System tab, there's a sub-menu with: User Account, Time Settings, Reboot/Reset, Backup & Restore (highlighted in red), and Firmware Update. The main content area is titled 'Backup & Restore' and is divided into two sections: 'Backup' and 'Restore'. The 'Backup' section has the text 'Save a copy of the current settings.' and a 'Backup' button. The 'Restore' section has the text 'Restore saved settings from a file.', a 'File:' label, a text input field, a 'Browse' button, and a 'Restore' button.

- To backup the configuration, click the button **Backup** in the Backup section, and the backup file will be saved to the host automatically.
- To restore the configuration, click the button **Browse** in the Restore section and choose the backup file from the host. Then click the button **Restore** to restore the configuration.

5.6 Update the Firmware

We occasionally provide the firmware update files for the EAP products on our official website. To get new functions of the EAP, you can check our official website and download the update files to update the firmware of your EAP.

To update the firmware, go to the **System > Firmware Update** page.



Follow the steps below to update the firmware of your EAP:

1. Go to our website <https://www.tp-link.com> and search your EAP model. Download the proper firmware file on the support page of the EAP.
2. Click the button **Browse**, locate and choose the correct firmware file from your host.
3. Click the button **Update** to update the firmware of the EAP. After updated, the EAP will be rebooted automatically.

Note:

The update process takes several minutes. To avoid damage to the EAP, please wait without any operation until the update is finished.

6

Application Example

This chapter provides an application example about how to establish and manage a EAP wireless network:

A restaurant wants to provide the wireless internet access for the employees and guests. The restaurant now has a router, a switch, a dual-band EAP and a computer. Follow the steps below to establish the wireless network:

1. *6.1 Determine the Network Requirements*

2. *6.2 Build the Network Topology*

3. *6.3 Log in to the EAP*

4. *6.4 Configure the EAP*

5. *6.5 Test the Network*

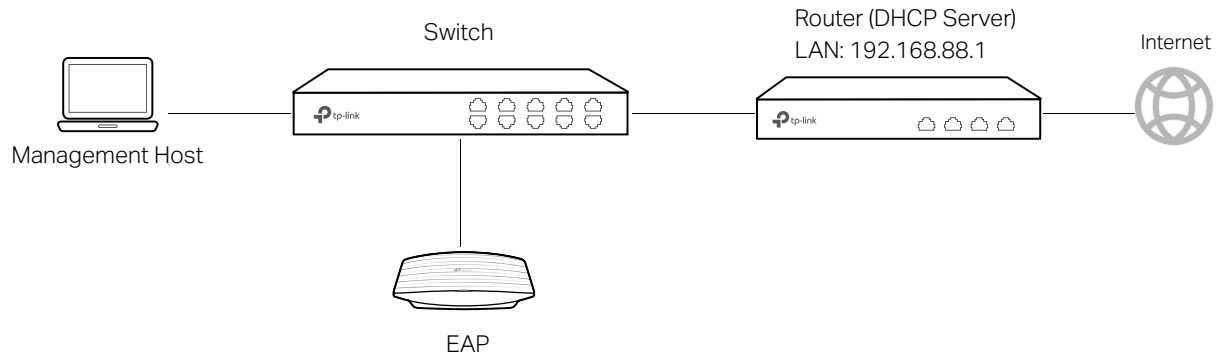
6.1 Determine the Network Requirements

Before starting to build the network, we need to first analyze and determine the network requirements. In this restaurant example, the network requirements are as follows:

- On both 2.4GHz and 5GHz bands, there are two SSIDs needed: one for the restaurant employees and one for the guests.
- In order to advertise the restaurant, the Portal feature needs to be configured on the SSIDs for the guests. In this way, the guests who have passed the portal authentication will be redirected to the restaurant's official website <http://www.restaurant1.com>.
- The employees of the restaurant can use the correct password to access the internet and do not need to pass the portal authentication. For security, the SSIDs for the employees should be encrypted with WPA2-PSK.
- To reduce power consumption, the Scheduler feature needs to be configured. The radio should operate only during the working time (9:00 am to 22:00 pm).

6.2 Build the Network Topology

Build the network topology as the following figure shows.



- The router is the gateway of the network and acts as a DHCP server to assign dynamic IP addresses to the management host, EAP and clients. The LAN IP of the router is 192.168.88.1/24.
- Connect the switch to the LAN port of the router.
- Connect the management host and the EAP to the switch. The IP address mode of the management host and EAP is dynamic, which means that they will get dynamic IP addresses from the router.

Tips:

If the router has more than one LAN port, we can also respectively connect the management host and the EAP to the LAN ports of the router.

6.3 Log in to the EAP

After building the network topology, follow the steps below to log in to the web page of the EAP:

1. On the management host, launch the web browser and enter "192.168.88.1" in the address bar. Then log in to the router and find the IP address of the EAP. As the following figure shows, the IP address of the EAP is 192.168.88.101.

LAN

DHCP

DHCP Client

DHCP Reservation

List of DHCP Client

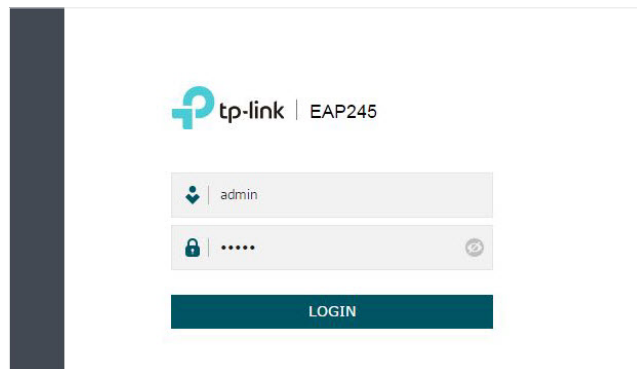
No.	Host Name	MAC Address	IP Address	Lease Time
1	EAP245-50-C7-BF	50-C7-BF-17-A6-E2	192.168.88.101	00:00:43
2	tplink2	F8-BC-12-9B-93-A4	192.168.88.100	00:00:58

Refresh

Search

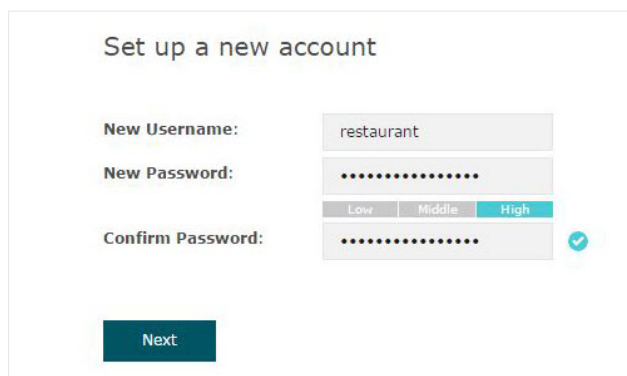
Help

2. Enter "192.168.88.101" in the address bar to load the login page of the EAP. Type the default username and password (both admin) in the two fields and click **LOGIN**.



The image shows the login page for a TP-Link EAP245 device. It features the TP-Link logo and the model name "EAP245". There are two input fields: one for the username, which contains "admin", and one for the password, which contains six dots. Below these fields is a dark blue button labeled "LOGIN".

3. In the pop-up window, specify a new username and a new password for the user account. Click **Next**.



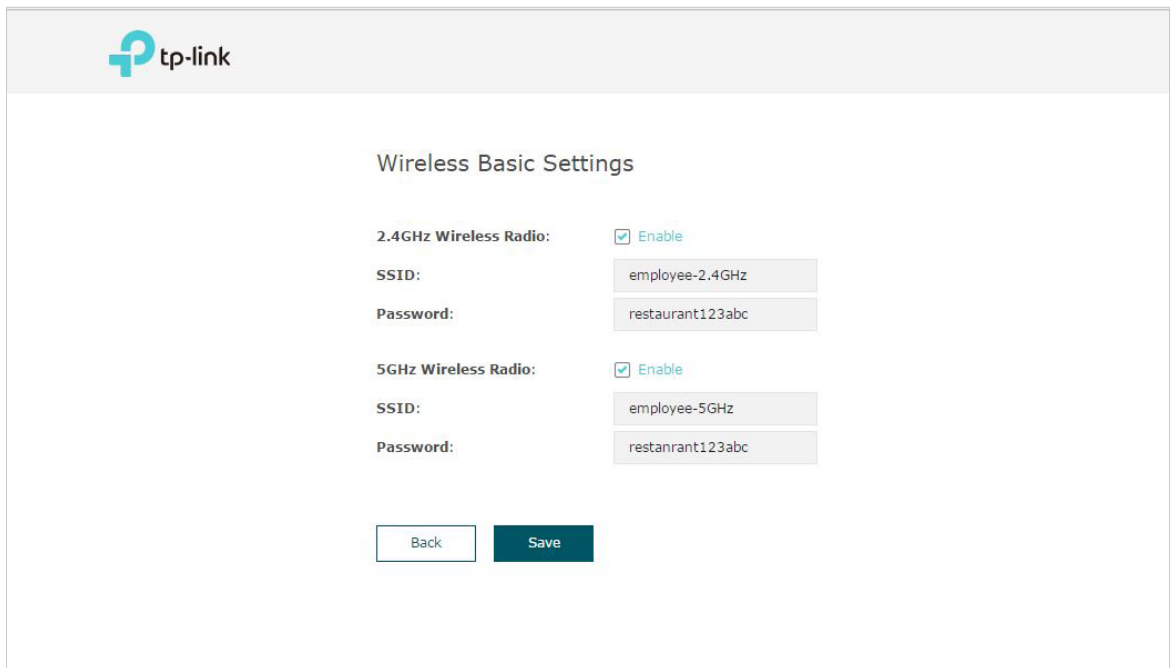
The image shows a "Set up a new account" page. It has three input fields: "New Username:" with the text "restaurant", "New Password:" with ten dots, and "Confirm Password:" with ten dots. To the right of the password fields are three tabs: "Low", "Middle", and "High", with "High" selected. A green checkmark icon is next to the "Confirm Password:" field. At the bottom is a dark blue button labeled "Next".

6.4 Configure the EAP

To achieve the network requirements in this application example, we need to [Configure SSIDs](#), [Configure Portal Authentication](#) and [Configure Scheduler](#).

Configure SSIDs

1. After Logging in to EAP, follow the step-by-step instructions to complete the basic configurations of creating SSIDs. Configure the **SSID** as "employee_2.4GHz" and "employee_5GHz", specify the **Password** as "restaurant123abc". Click **Save**.



tp-link

Wireless Basic Settings

2.4GHz Wireless Radio: ☒ Enable

SSID: employee-2.4GHz

Password: restaurant123abc

5GHz Wireless Radio: ☒ Enable

SSID: employee-5GHz

Password: restanrant123abc

Back Save

2. Go to the **Wireless > Wireless Settings** page. Create SSIDs for guests on 2.4GHz. Click  **Add** to add a new SSID.

2.4GHz SSIDs							 Add
ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action	
1	employee-2.4GHz	0	Enable	WPA-PSK	Disable	 	

3. The following page will appear. Configure this SSID as "guest_2.4GHz", keep the **Security Mode** as "None" and check the box to enable the **Portal** feature for this SSID. Click **OK**.

2.4GHz SSIDs

SSID:

guest-2.4GHz

SSID Broadcast:

☒ Enable

Security Mode:

None

Guest Network:

☐ Enable

Rate Limit:

☐ Enable

OK

Cancel

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
--	--	--	--	--	--	--
1	employee-2.4GHz	0	Enable	WPA-PSK	Disable	

4. Click

2.4GHz

5GHz

 to enter the configuration page for the 5GHz band. Similarly to the configurations for the 2.4GHz band, configure another SSID for the guests on the 5GHz band.

Configure Portal Authentication

Follow the steps below to configure portal authentication:

1. Go to the **Wireless > Portal** page.

2. Configure the portal feature as the following figure shows.

The screenshot shows the TP-Link web portal configuration interface. The top navigation bar includes the TP-Link logo and icons for help and search. Below this is a main menu with tabs for Status, Wireless (selected), Management, and System. Under the Wireless tab, there are sub-tabs for Wireless Settings, Portal (selected), VLAN, MAC Filtering, Scheduler, Band Steering, QoS, and Rogue AP Detection. The main content area is titled 'Portal Configuration' and contains the following settings:

- SSID:** guest-2.4GHz, guest-5GHz
- Authentication Type:** Local Password
- Password:** restaurant123
- Authentication Timeout:** Custom (0 D 2 H 0 M)
- Redirect:** ☒ Enable
- Redirect URL:** http://restaurant1.com
- Portal Customization:** Local Web Portal

The 'Local Web Portal' customization preview shows a login page with the following elements:

- Welcome to XXX restaurant
- Password input field
- Term of Use section:
 - By using the provided internet, you agree to these terms:
 - 1.xxxxxxx
 - 2.xxxxxxxxxx
- ☒ I accept the Term of Use
- Login button

A 'Save' button is located at the bottom left of the configuration area.

- 1) Select the SSIDs for the guests on which the portal will take effect.
- 2) Select the **Authentication Type** as "Local Password" and specify the **Password** as "restaurant123".
- 3) Configure **Authentication Timeout**. Here we customize the timeout as 2 hours. It means that guests will be logged out after they have been authenticated for 2 hours. To continue to use the internet service, these guests need to enter the password to pass the portal authentication once again.
- 4) Check the box to enable **Redirect**, and enter the website of the restaurant: **http://www.restaurant1.com**.

- 5) Configure the authentication page. Specify the title and the term of use. To access the internet, guests need to enter the correct password in the **Password** field, accept the **Term of Use**, and click the **Login** button.

3. Click **Save**.

Configure Scheduler

Follow the steps below to schedule the radio to operate only during the working time (9:00 am to 22:00 pm).

1. Go to the **Wireless > Scheduler** page.
2. In the **Settings** section, check the box to enable **Scheduler**, and select the **Association Mode** as "Associated with AP". Click **Save**.

Settings

Scheduler: ☒ Enable

Association Mode: Associated with AP ▼

Save

3. In the **Scheduler Profile Configuration** section, click  **Create Profiles**.

Scheduler Profile Configuration

 Create Profiles

- 1) The following page will appear. Click  **Add a Profile** and specify the profile name as "worktime". Click **OK**.

Scheduler Profile Configuration

 Add a Profile

Profile Name	Modify
--	--

Profile:

Cancel OK

 Add an item

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--

- 2) Choose the newly added profile "worktime", and click  **Add an item**. Then the item configuraiton page will appear. Specify the time range as everyday 9:00 to 22:00. Click **OK**.

Scheduler Profile Configuration

 Add a Profile

Profile Name	Modify
worktime	 



 Add an item

ID	Profile Name	Days	Start Time	End Time	Modify
--	--	--	--	--	--

Day:

☐ Weekday ☐ Weekend ☒ Every Day ☐ Custom

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

☒ Sun

Time: ☐ 24 hours

Start Time: 09 : 00

End Time: 22 : 00

Cancel

OK

4. In the **Scheduler Association** section, select "worktime" in the **Profile Name** column and select "Radio On" in the **Action** column. Click **Save**.

Scheduler Association

ID	AP	AP MAC	Profile Name	Action
1	EAP245-50-c7-bf-17-a6-e2	50-C7-BF-17-A6-E2	worktime	Radio On

Save

111

6.5 Test the Network

To ensure that the employees and guests can surf the internet via the wireless network, we can use a client device, such as a telephone, to test whether the SSIDs are working normally.

- To test the SSIDs for the employees, follow the steps below:
 - 1) Enable the Wi-Fi feature of the client device.
 - 2) Choose the SSID "employee_2.4GHz" or "employee_5GHz" among the detected SSIDs.
 - 3) Enter the password "restaurant123abc" to join the wireless network.
 - 4) Check whether internet websites can be visited successfully.
- To test the SSIDs for the guests, follow the steps below:
 - 1) Enable the Wi-Fi feature of the client device.
 - 2) Choose the SSID "guest_2.4GHz" or "guest_5GHz" among the detected SSIDs.
 - 3) The default web browser on the device will pop up and the authentication page will appear. Enter the password "restaurant123", check the box to accept the term of use, and click the **LOGIN** button.

