Configuring the EAPs Globally via Omada Controller

CHAPTERS

This guide applies to:

Omada Controller 3.2.1.

This chapter introduces the global configurations applied to all the managed EAPs. To configure a specific EAP, please refer to Configuring the EAPs Separately via Omada Controller.

In global configurations, you can configure the following items:

1. Wireless Network
2. Access Control
3. Portal Authentication
4. Free Authentication Policy
5. MAC Filter
6. Scheduler
7. QoS
8. Site Settings

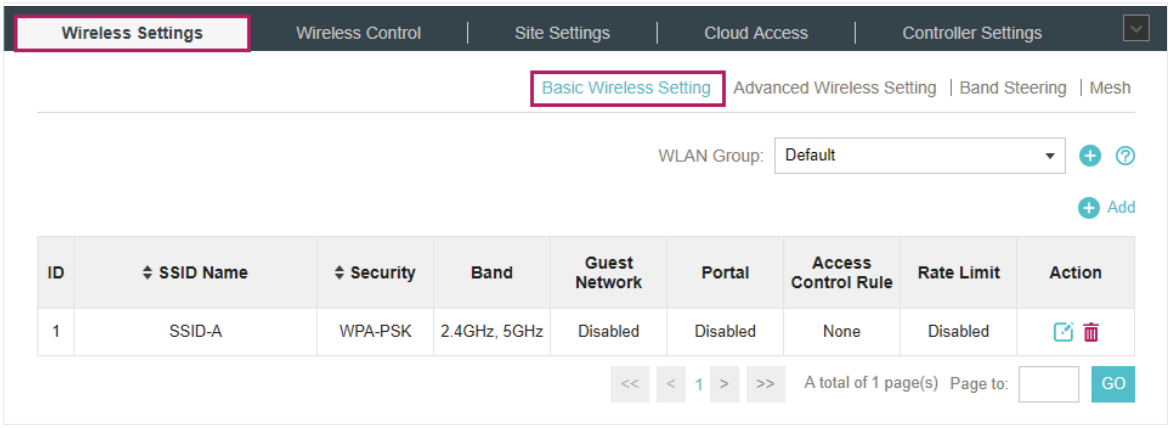
1 Wireless Network

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

1.1 Add Wireless Networks

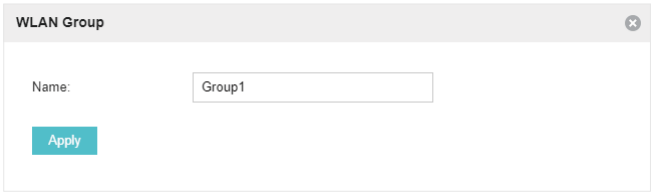
To add wireless networks, follow the steps below.

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



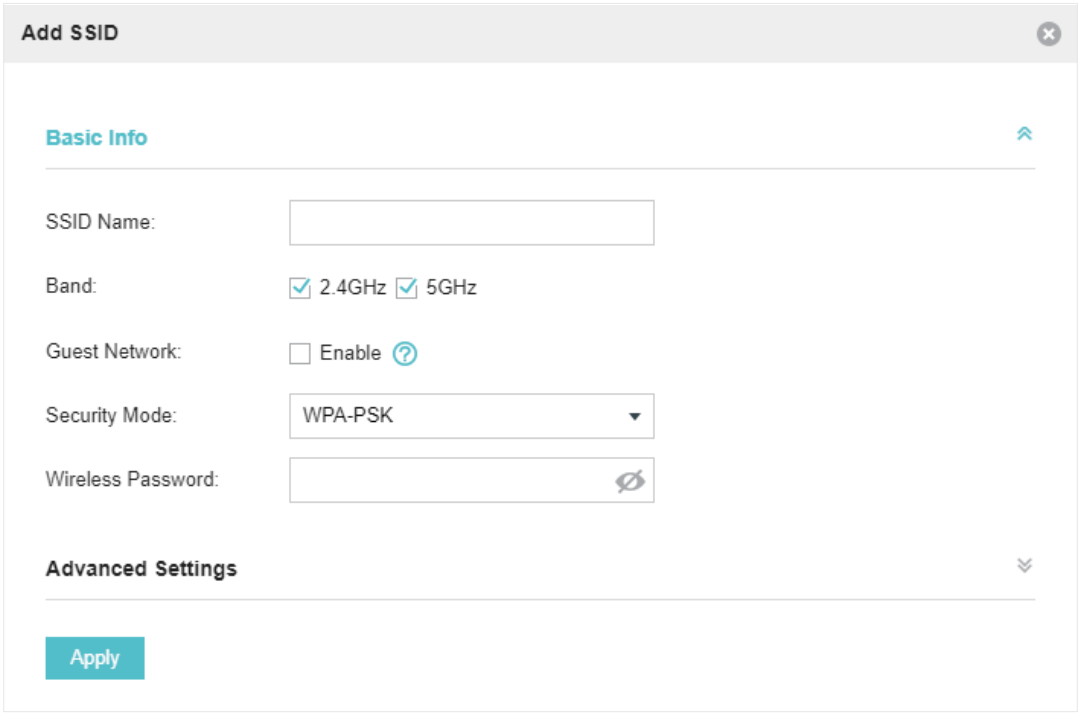
2. Click at the right of  to add a WLAN group. Creating WLAN groups is an easy way to quickly deploy EAPs by creating a template-based set of SSIDs with wireless parameters. Different WLAN groups can be applied to different EAPs. If you have no need to group your wireless networks, you can use the default WLAN group and skip this step.

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



4. Select the WLAN group  and click  to add an SSID to the specific WLAN group.

5. Configure the parameters in the following window.



SSID Name	Enter an SSID name using up to 32 characters.
Band	Select the radio band to add the SSID.
Guest Network	With this option enabled, the network act as a guest network. All the clients connecting to the SSID will be blocked from reaching any private IP subnet.
Security Mode	Select the security mode of the wireless network. None: The hosts can access the wireless network without authentication. WEP/WPA-Enterprise/WPA-PSK: The hosts need to get authenticated before accessing the wireless network. For the network security, you are suggested to encrypt your wireless network. Settings vary in different security modes and the details are in the following introduction.

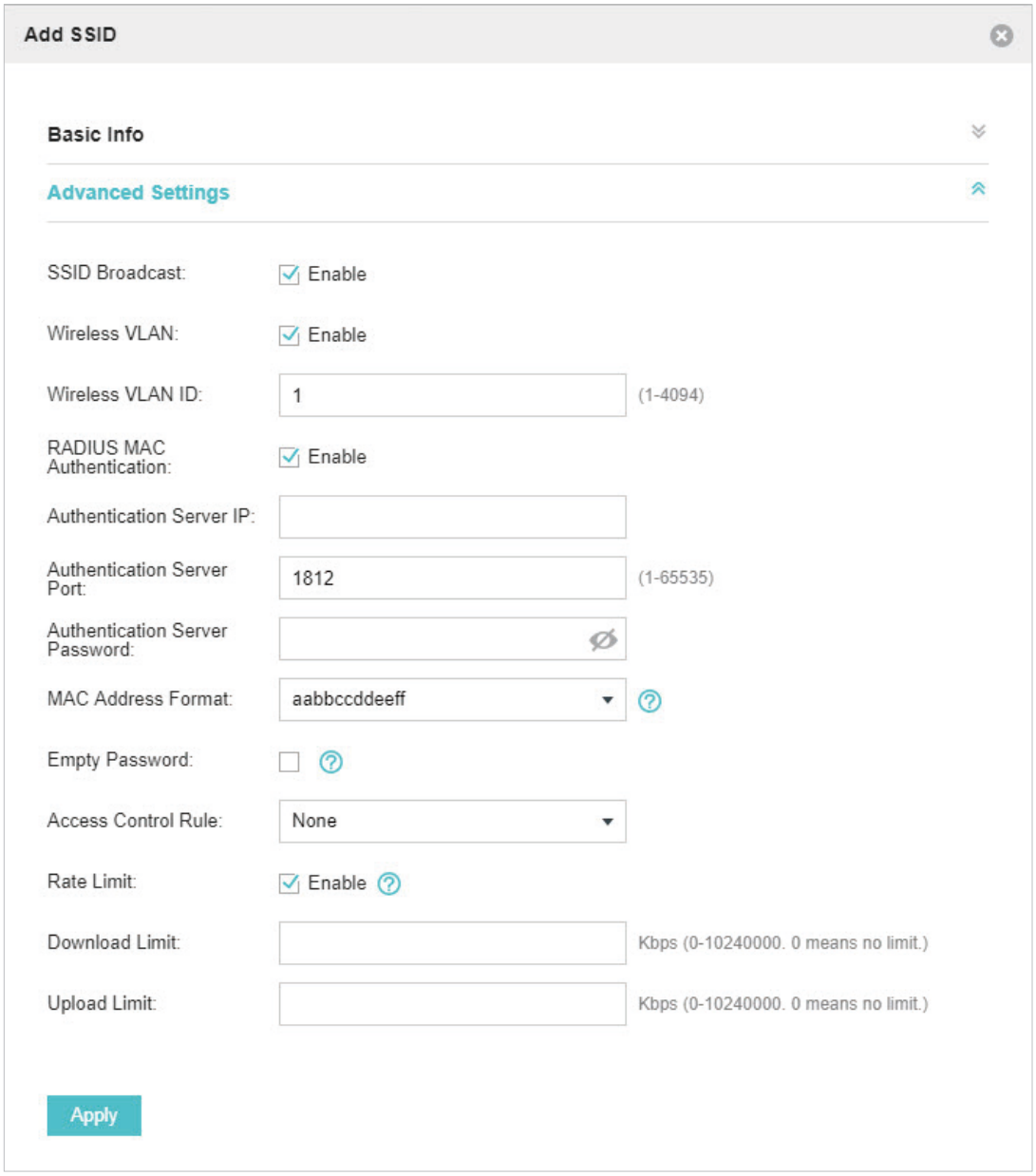
Note:

- 8 SSIDs can be created on each band at most.
- The SSID on different radio band with the same name will be regarded as an identical SSID entry. When you upgrade your controller or restore the backup files from the controller with the version 3.0.5 or below, the SSID entries with the same name will be merged if they are on 2.4GHz and 5GHz in the same WLAN group. All the configurations in the entry will be changed to the parameters of the original SSID on the 2.4GHz radio band.

Following is the detailed introduction of None, WEP, WPA-Enterprise and WPA-PSK.

None

The hosts can access the wireless network without authentication. Configure th advanced parameters in the following window.



SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP. The option is enabled by default.

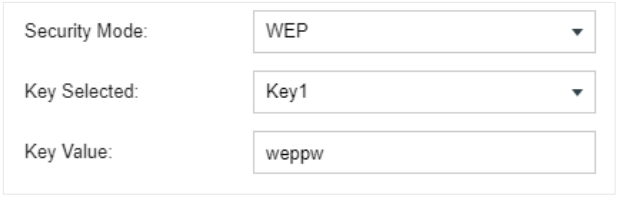
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other. To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the **Wireless VLAN ID**.
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
RADIUS MAC Authentication	With this option enabled, the EAP will send the MAC address of the client to the RADIUS server as the username and password for authentication. If the authorization succeeds, the RADIUS server grants the client access to the network. To set RADIUS MAC Authentication, enable the option and configure the following parameters: **Authentication Server IP**, **Authentication Server Port**, **Authentication Server Password**, **MAC Address Format**, and **Empty Password**.
Authentication Server IP	With RADIUS MAC Authentication enabled, enter the IP address of the authentication server.
Authentication Server Port	With RADIUS MAC Authentication enabled, enter the port number you have set on the RADIUS server for authentication requests. The default setting is 1812.
Authentication Server Password	With RADIUS MAC Authentication enabled, enter the authentication password. The authentication server and the controller use the password to encrypt passwords and exchange responses.
MAC Address Format	With RADIUS MAC Authentication enabled, select the format to convert a client's MAC address to the RADIUS username.
Empty Password	With the option enabled, a blank password for RADIUS MAC Authentication will be allowed. With the option disabled, the password will be the same as the username.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details. Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.

WEP

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

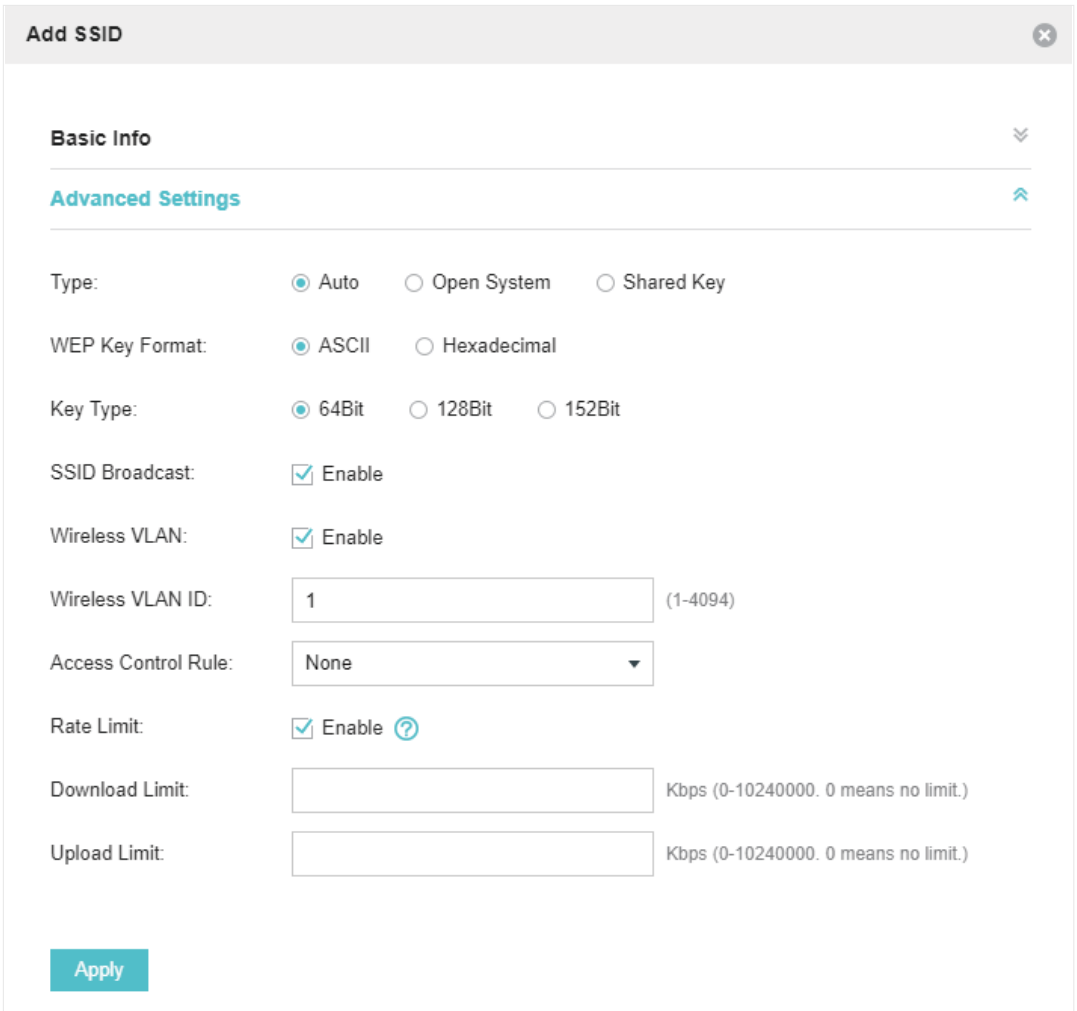
Note:

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



Key Selected	Select one key to specify. You can configure four keys at most.
Key Value	Enter the WEP keys. The length and valid characters are affected by key type.

Configure th advanced parameters in the following window.

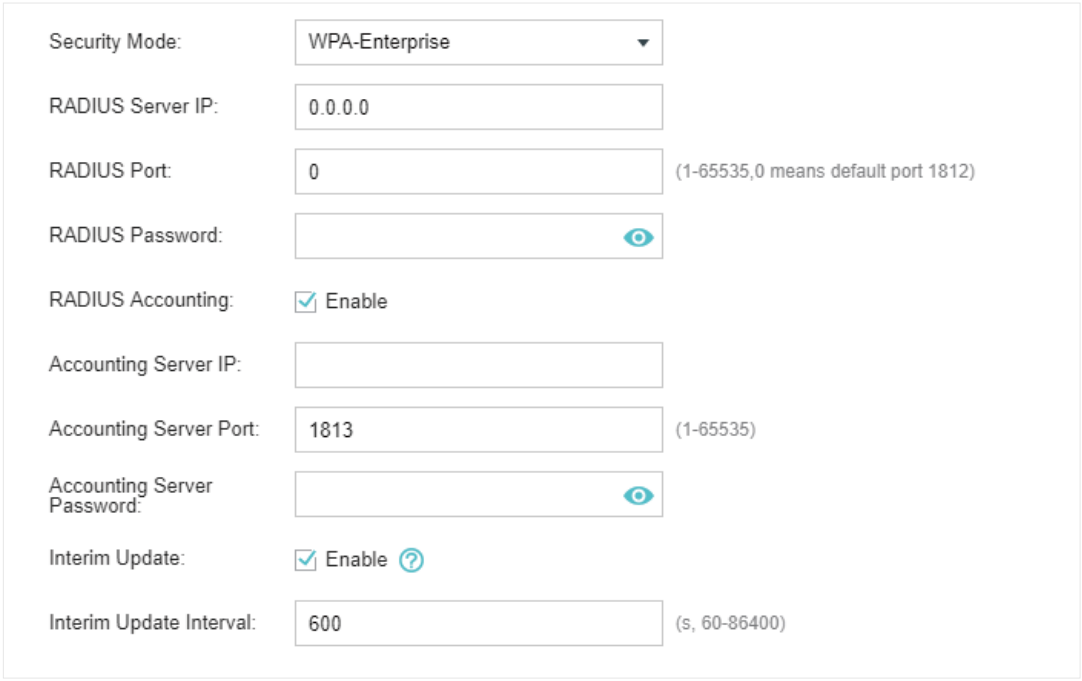


Type	Select the authentication type for WEP. **Auto**: The Omada Controller can select Open System or Shared Key automatically based on the wireless station's capability and request. **Open System**: Clients can pass the authentication and associate with the wireless network without password. However, correct password is necessary for data transmission. **Shared Key**: Clients have to input password to pass the authentication, otherwise it cannot associate with the wireless network or transmit data.
WEP Key Format	Select **ASCII** or **Hexadecima** as the WEP key format. **ASCII**: ASCII format stands for any combination of keyboard characters of the specified length. **Hexadecimal**: Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) with the specified length.
Key Type	Select the WEP key length for encryption. **64Bit**: Enter 10 hexadecimal digits or 5 ASCII characters. **128Bit**: Enter 26 hexadecimal digits or 13 ASCII characters. **152Bit**: Enter 32 hexadecimal digits or 16 ASCII characters.
Key Value	Enter the WEP keys. The length and valid characters are affected by key type.
SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP. The option is enabled by default.
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other. To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the **Wireless VLAN ID**.
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.

Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details. Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.

WPA-Enterprise

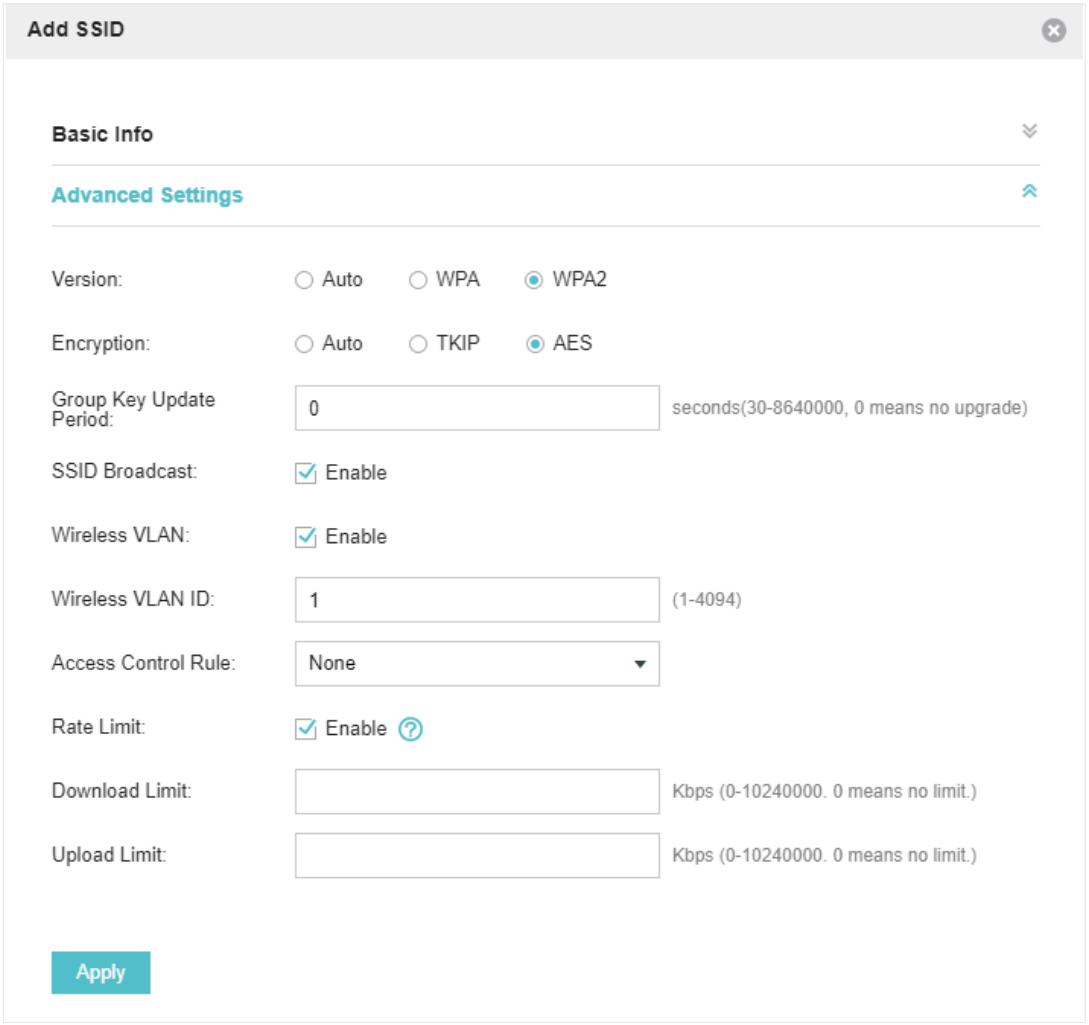
The WPA-Enterprise mode requires a RADIUS server to authenticate clients. Since the WPA-Enterprise can generate different passwords for different clients, it is much safer than WPA-PSK. However, it costs much more to maintain and is usually used by enterprise.



RADIUS Server IP	Enter the IP address of the RADIUS Server.
RADIUS Port	Enter the port number of the RADIUS Server.
RADIUS Password	Enter the shared secret key of the RADIUS server.
RADIUS Accounting	Enable or disable RADIUS Accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server.

Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled. Enter the appropriate duration between updates for EAPs in **Interim Update Interval**.
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.

Configure th advanced parameters in the following window.



Version	Select the version of WPA-Enterprise. **Auto**: The EAP will automatically choose the version used by each client device. **WPA/WPA2**: Two versions of Wi-Fi Protected Access.

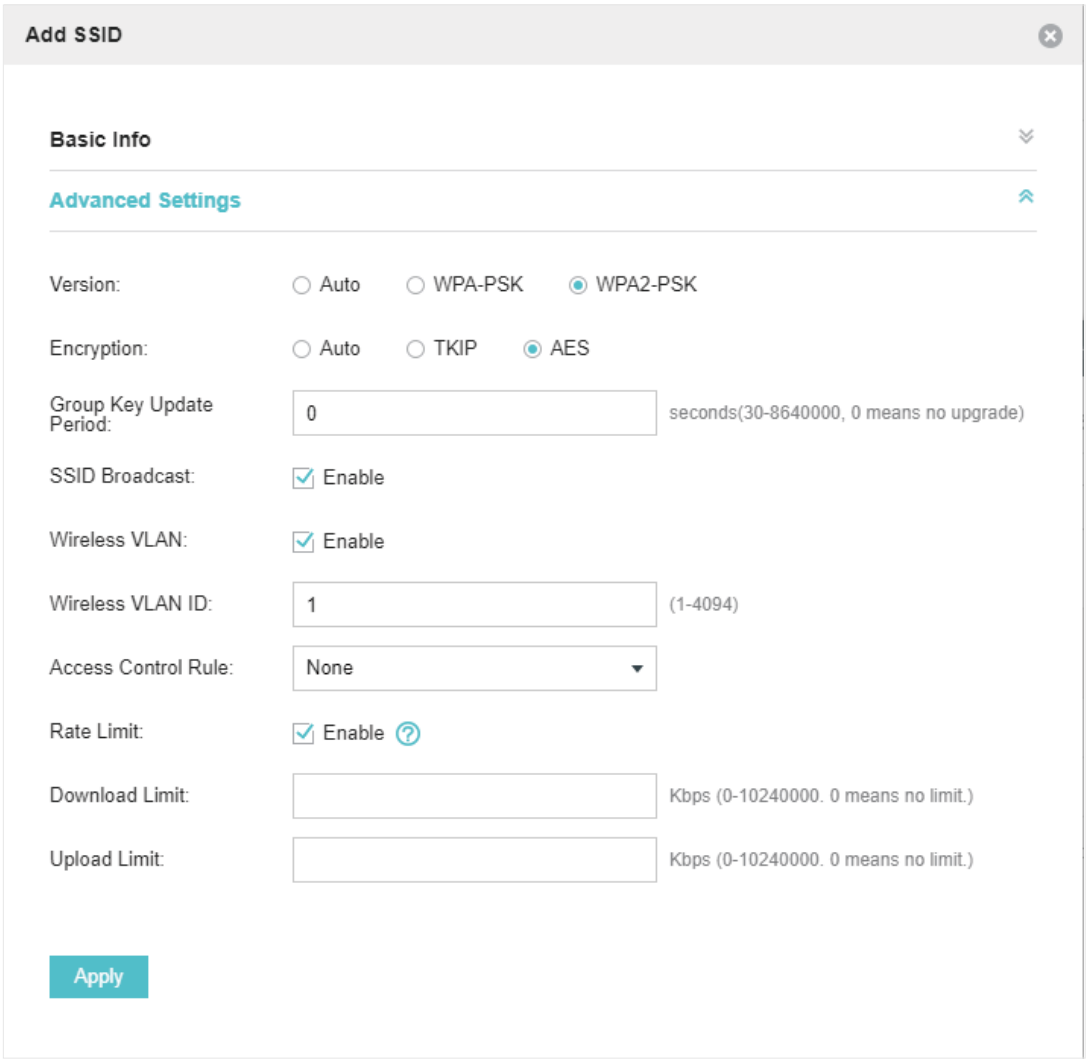
Encryption	Select the Encryption type. **Auto**: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client device's request. **TKIP**: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network of the EAP. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES**: Advanced Encryption Standard. We recommend that you select AES as the encryption type because it is more secure than TKIP.
Group Key Update Period	Specify a group key update period, which instructs the EAP how often it should change the encryption keys. The value can be either 0 or 30~8640000 seconds. 0 means no change of the encryption key anytime.
SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP. The option is enabled by default.
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other. To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the **Wireless VLAN ID**.
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details. Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.

WPA-PSK

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

Wireless Password	Configure the wireless password with ASCII or Hexadecimal characters. For ASCII, the length should be between 8 and 63 characters with combination of numbers, letters (case-sensitive) and common punctuations. For Hexadecimal, the length should be 64 characters (case-insensitive, 0-9, a-f, A-F).

Configure th advanced parameters in the following window.



Version	Select the version of WPA-Enterprise. **Auto**: The EAP will automatically choose the version used by each client device. **WPA/WPA2**: Two versions of Wi-Fi Protected Access.

Encryption	Select the Encryption type. **Auto**: The default setting is Auto and the EAP will select TKIP or AES automatically based on the client request. **TKIP**: Temporal Key Integrity Protocol. TKIP is not supported in 802.11n mode, 802.11ac mode or 802.11n/ac mixed mode. If TKIP is applied in 802.11n, 802.11 ac or 802.11n/ac mixed mode, the clients may not be able to access the wireless network of the EAP. If TKIP is applied in 11b/g/n mode (2.4GHz) or 11a/n mode(5GHz), the device may work at a low transmission rate. **AES**: Advanced Encryption Standard. We recommend that you select AES as the encryption type for it is more secure than TKIP.
Group Key Update Period	Specify a group key update period, which instructs the EAP how often it should change the encryption keys. The value can be either 0 or 30~8640000 seconds. 0 means the encryption keys will not be changed all the time.
SSID Broadcast	With the option enabled, EAPs will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the EAP. The option is enabled by default.
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other. To set a wireless VLAN for the wireless network, enable the option and set a VLAN ID in the **Wireless VLAN ID**.
Wireless VLAN ID	Enter a VLAN ID for the wireless VLAN. Wireless networks with the same VLAN ID are grouped to a VLAN. The value ranges from 1 to 4094.
Access Control Rule	Select an Access Control rule for this SSID. For more information, refer to Access Control.
Rate Limit	With this option enabled, the download and upload rate of each client which connects to the SSID will be limited to balance bandwidth usage. You can limit the download and upload rate for some specific clients by configuring rate limit in client list, refer to Manage Clients in the Action Column to get more details. Note that the download and upload rate will be limited to the minimum of the value configured in SSID, client and portal configuration.
Download Limit	With Rate Limit enabled, specify the limit of download rate. 0 means unlimited.
Upload Limit	With Rate Limit enabled, specify the limit of upload rate. 0 means unlimited.

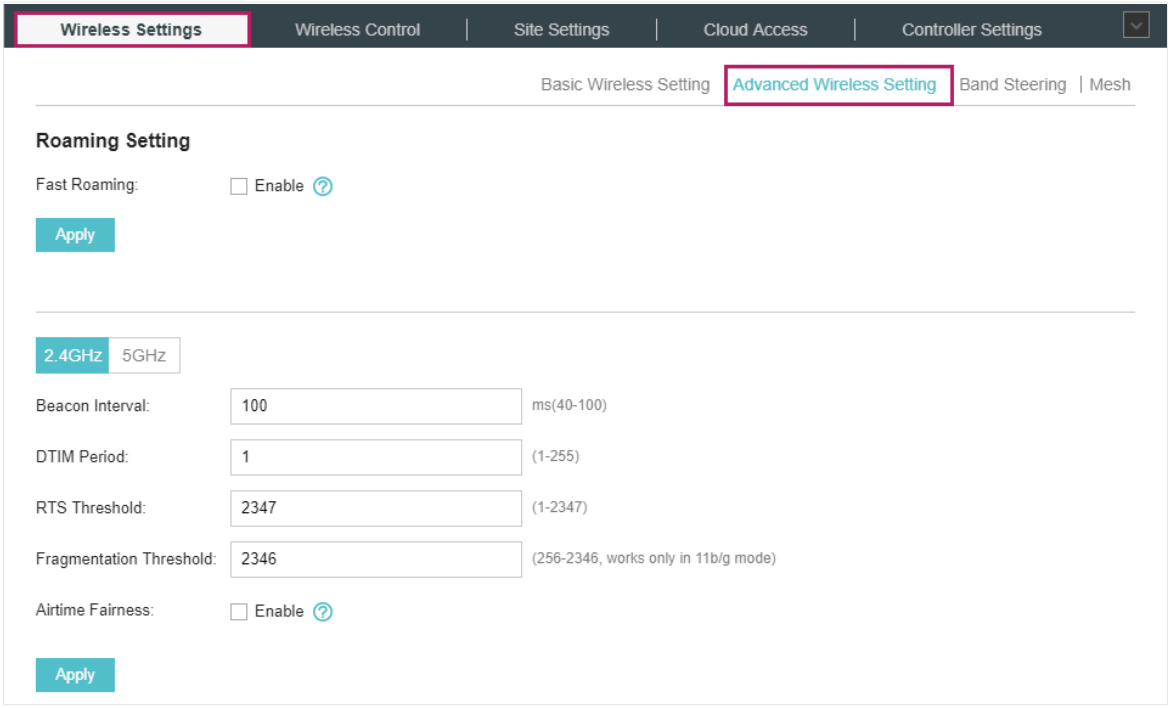
6. Click **Apply**.

1.2 Configure Advanced Wireless Parameters

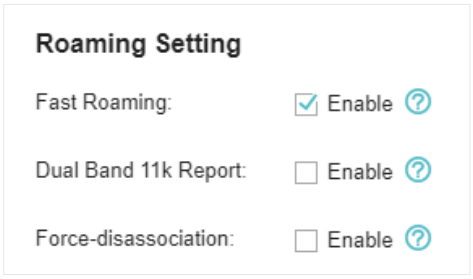
Proper wireless parameters can improve the network's stability, reliability and communication efficiency. The advanced wireless parameters consist of **Fast Roaming**, **Beacon Interval**, **DTIM Period**, **RTS Threshold**, **Fragmentation Threshold** and **Airtime Fairness**.

To configure the advanced wireless parameters, follow the steps below.

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

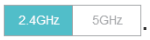


2. Enable **Fast Roaming** and configure the corresponding parameters.



Fast Roaming	With this option enabled, 11k/v capable clients can have improved fast roaming experience when moving among different APs.
Dual Band 11k Report	With this feature disabled, the controller provides candidate AP report that contains the APs in the same band as the clients. With this feature enabled, the controller provides candidate AP report that contains the APs in both 2.4GHz and 5GHz bands.

Force-disassociation	The controller dynamically monitors the link quality of every associated client. When the client's current link quality drops below the predefined threshold and there are some other APs with better signal, the current AP issues an 11v roaming suggestion to the client. With Force-disassociation disabled, the AP only issues a roaming suggestion, but whether to roam or not is determined by the client. With Force-disassociation enabled, the AP not only issues a roaming suggestion but also disassociates the client after a while. Thus the client is supported to re-associate to a better AP. This function is recommended when there are sticky clients that don't roam.

3. Click **Apply**.
4. Select the band frequency 

.
5. Configure the following parameters.

Beacon Interval	Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients. **Beacon Interval** value determines the time interval of the beacons sent by the device. You can specify a value between 40 and 100ms. The default is 100ms.
DTIM Period	The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the EAP has buffered data for client devices. The **DTIM Period** indicates how often the clients served by this EAP should check for buffered data still on the EAP awaiting pickup. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating clients check for buffered data on the EAP at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend that you keep it by default.
RTS Threshold	RTS (Request to Send) can ensure efficient data transmission. When RTS is activated, the client will send a RTS packet to EAP to inform that it will send data before it send packets. After receiving the RTS packet, the EAP notices other clients in the same wireless network to delay their transmitting of data and informs the requesting client to send data, thus avoiding the conflict of packet. If the size of packet is larger than the **RTS Threshold**, the RTS mechanism will be activated. If you specify a low threshold value, RTS packets are sent more frequently and help the network recover from interference or collisions that might occur on a busy network. However, it also consumes more bandwidth and reduces the throughput of the packet. We recommend that you keep it by default. The recommended and default value is 2347.

Fragmentation Threshold	The fragmentation function can limit the size of packets transmitted over the network. If a packet exceeds the **Fragmentation Threshold**, the fragmentation function is activated and the packet will be fragmented into several packets. Fragmentation helps improve network performance if properly configured. However, too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.
Airtime Fairness	With this option enabled, each client connecting to the EAP can get the same amount of time to transmit data, avoiding low-data-rate clients to occupy too much network bandwidth and improving the network throughput. We recommend that you enable this function under multi-rate wireless networks.

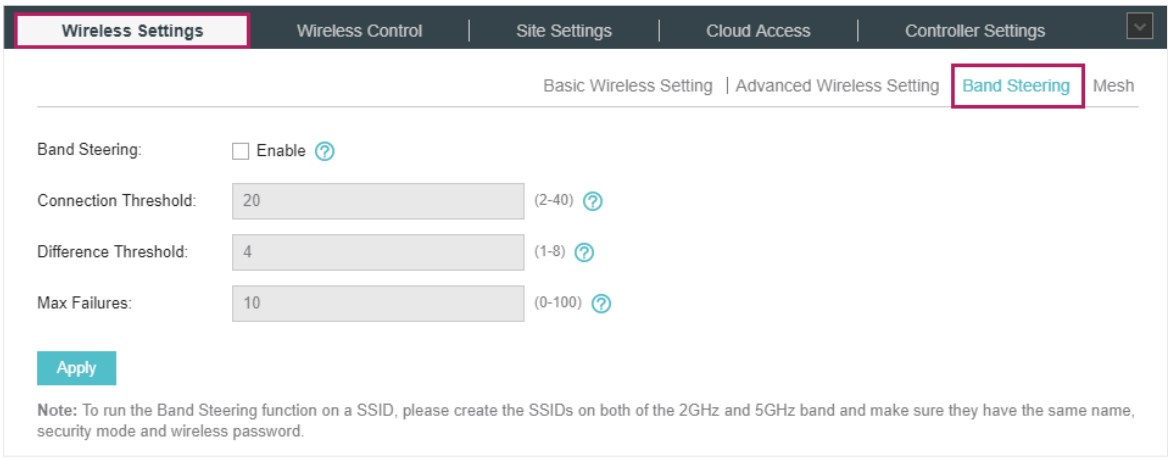
6. Click **Apply**.

1.3 Configure Band Steering

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

To configure Band Steering, follow the steps below.

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



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

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

Connection Threshold/ Difference Threshold	**Connection Threshold** defines the maximum number of clients connected to the 5GHz band. The value of **Connection Threshold** is from 2 to 40, and the default is 20. **Difference Threshold** defines the maximum difference between the number of clients on the 5GHz band and 2.4GHz band. The value of **Difference Threshold** is from 1 to 8, and the default is 4. When the following two conditions are both met, the EAP prefers to refuse the connection request on 5GHz band and no longer steers other clients to the 5GHz band: 1. The number of clients on the 5GHz band reaches the **Connection Threshold** value. 2. The difference between the number of clients on the 2.4GHz band and 5GHz band reaches the **Difference Threshold** value.
Max Failures	If a client repeatedly attempts to associate with the EAP on the 5GHz band and the number of rejections reaches the value of **Max Failures**, the EAP will accept the request. The value is from 0 to 100, and the default is 10.

4. Click **Apply**.

1.4 Configure Mesh

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

Note:

- EAP225-Outdoor with specific firmware (version 1.3 or above) and EAP225 V3 with specific firmware (version 2.5.0 or above) are available for mesh function currently.
- Only the EAPs in the same site can establish a mesh network.

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

- Root AP: The AP is managed by Omada Controller with a wired data connection that can be configured to relay data to and from mesh APs (Downlink AP).

- Isolated AP: When the EAP which has been managed before by Omada Controller connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.

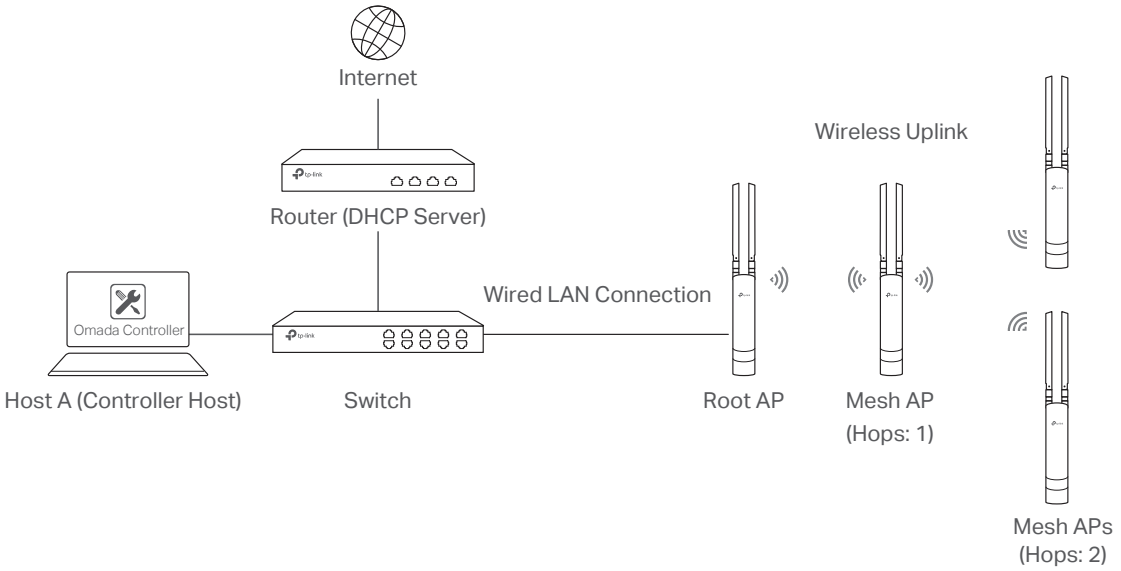
- Mesh AP: An isolated AP will be mesh AP after establishing a wireless connection to the AP with network access.

- Uplink AP/Downlink AP: Among mesh APs, the AP that offers the wireless connection for other APs is Uplink AP. A Root AP or an intermediate AP can be the Uplink AP. And the AP that connects to the Uplink AP is called Downlink AP. An uplink AP can offer direct wireless connection for 4 Downlink APs at most.

- Wireless Uplink: The action that a Downlink AP connects to the uplink AP.

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

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



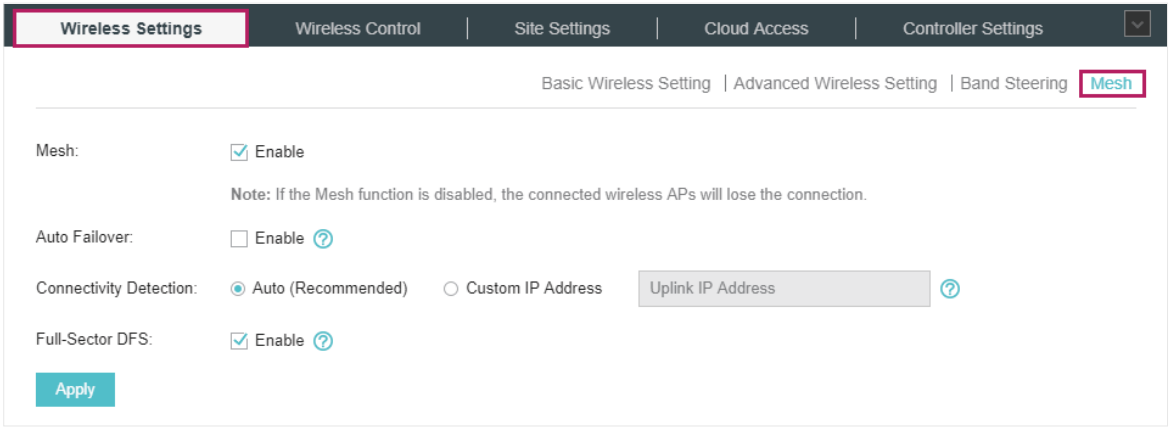
After all the EAPs are adopted, a mesh network is established. Then the EAPs connected to the network wirelessly also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

To establish a mesh network, follow the steps below.

- Enable Mesh Function.

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

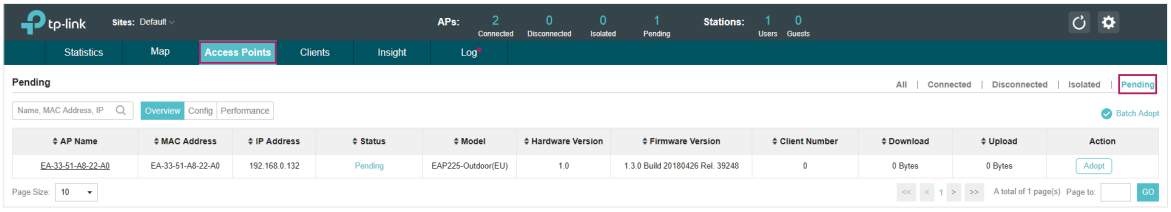
1. Go to **Wireless Settings > Mesh**.



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

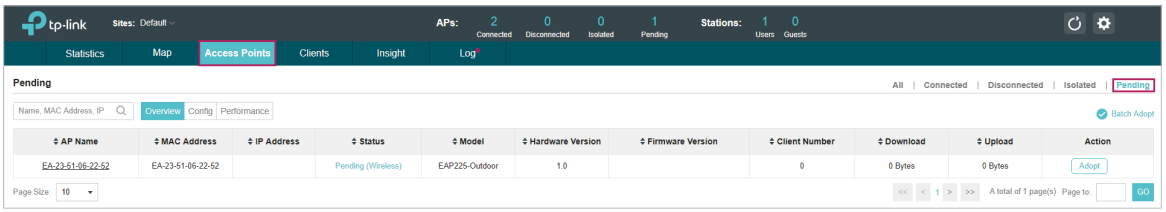
Auto Failover	Enable or disable Auto Failover. Auto Failover is used to automatically maintain the mesh network for the controller. With this feature enabled, the controller can automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. Thus the controller will automatically select a new uplink AP for the mesh EAPs when the original uplink fails.
Connectivity Detection	Specify the method of Connection Detection. In a mesh network, the APs can send ARP request packets to a fixed IP address to test the connectivity. If the link fails, the status of these APs will change to Isolated. **Auto (Recommended):** Select this method and the mesh APs will send ARP request packets to the default gateway for the detection. **Custom IP Address:** Select this method and specify a desired IP address. The mesh APs will send ARP request packets to the custom IP address to test the connectivity. If the IP address of the AP is in different network segments from the custom IP address, the AP will use the default gateway IP address for the detection.
Full-Sector DFS	With this feature enabled, when radar signals are detected on current channel by one EAP, the other EAPs in the mesh network will be also informed. Then all EAPs in the mesh network will switch to an alternate channel.

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



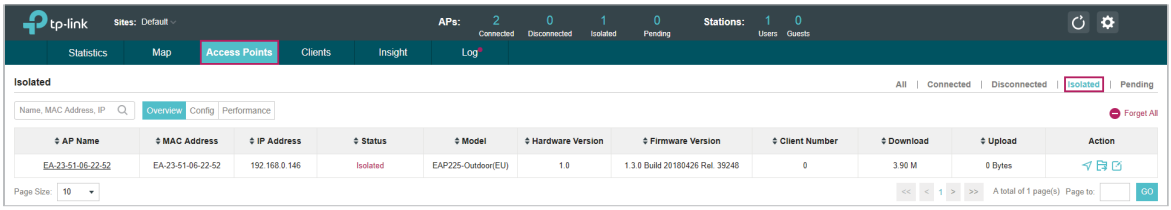
6. Install the EAP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The EAPs that is waiting for Wireless Uplink includes two cases: factory default EAPs and EAPs that has been managed by Omada Controller before.

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

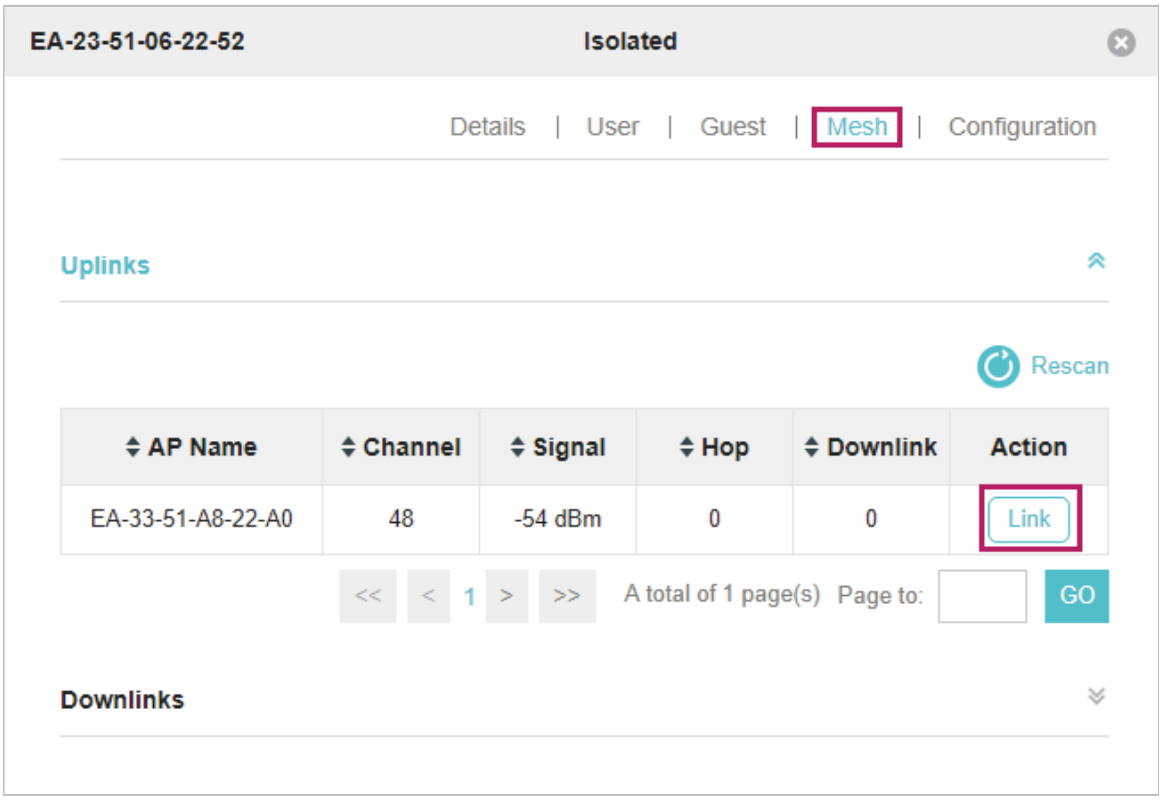


After adoption begins, the status of Pending (Wireless) EAP will become Adopting (Wireless) and then Connected (Wireless). It should take roughly 2 minutes to show up Connected (Wireless) within your controller.

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



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



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

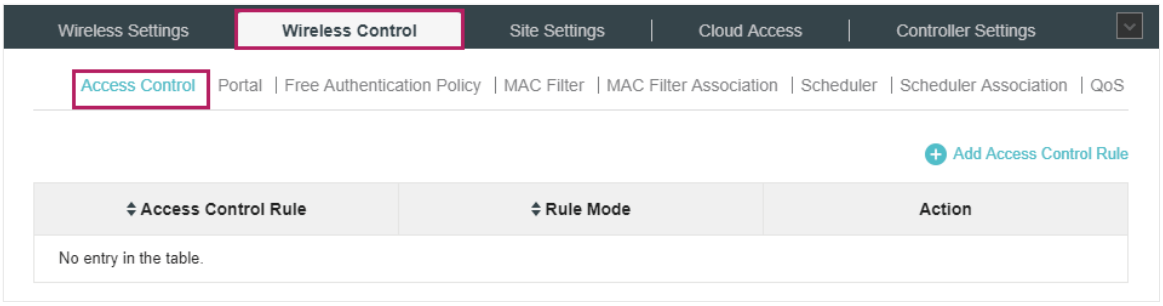
Note:

- You can manually select the uplink AP that you want to connect in the uplink EAP list. To build a mesh network with better performance, we recommend that you select the Uplink AP with the strongest signal, least hop and least Downlink AP.
- You can enable **Auto Failover** to make the controller automatically select an uplink AP for the isolated EAP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh EAPs when the original uplink fails.

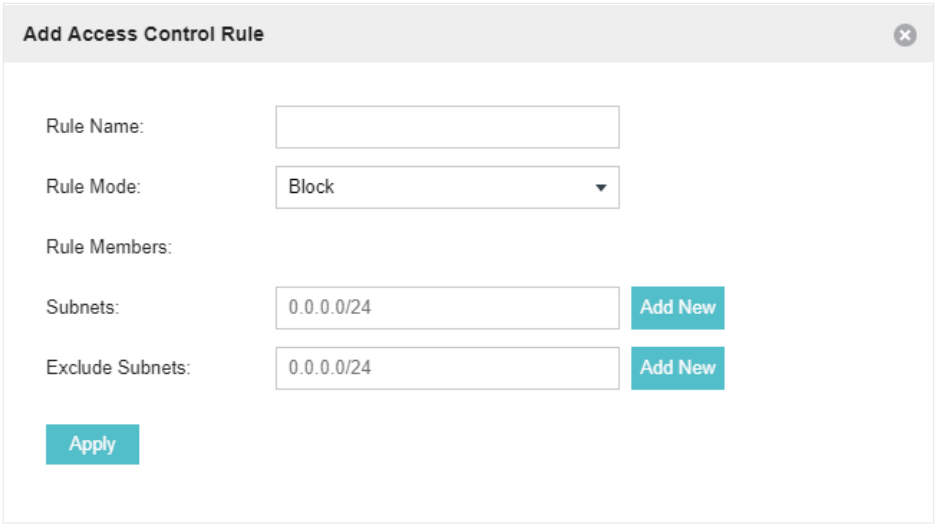
2 Access Control

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

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



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



3. Configure the following parameters.

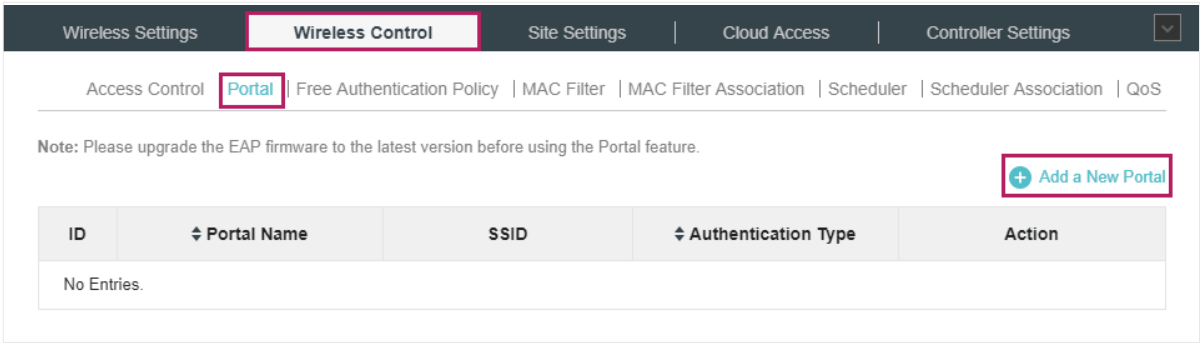
Rule Name	Specify a name for this rule.
Rule Mode	Select the mode for this rule. **Block**: Select this mode to block clients to access the specific subnets. **Allow**: Select this mode to allow clients to access the specific subnets.
Rule Members	Specify the member subnets for this rule. **Subnets**: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

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

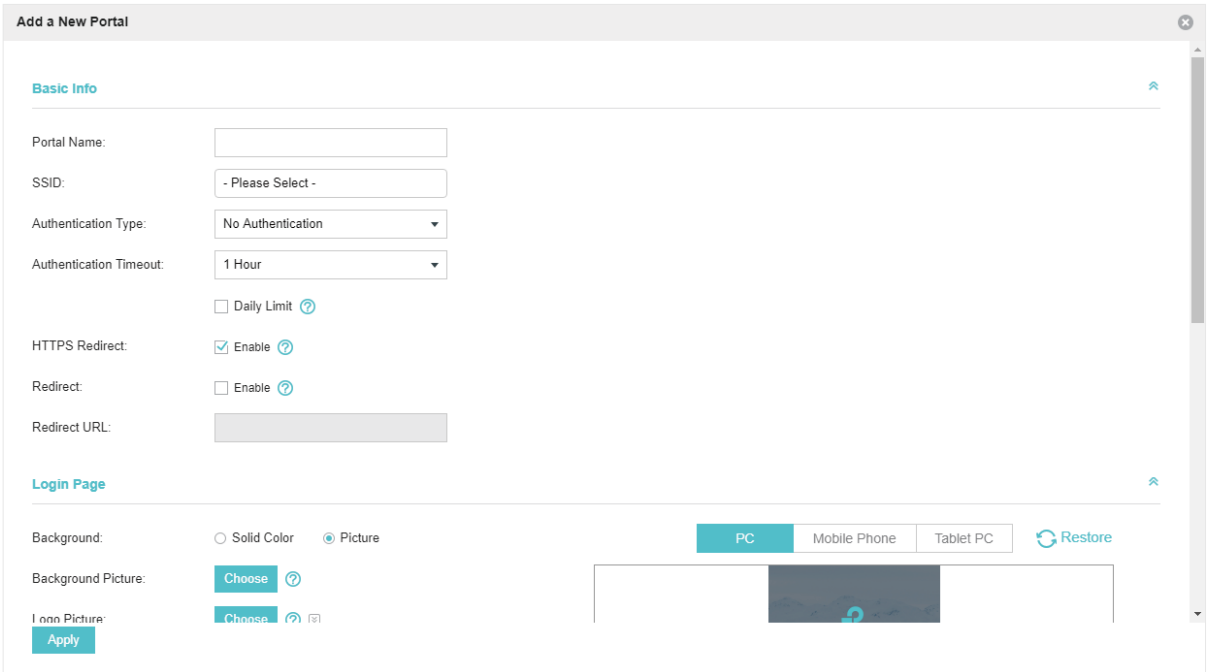
3 Portal Authentication

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

To configure Portal Authentication, go to **Wireless Control > Portal and click** Add a New Portal **.**



Then the following window will pop up:



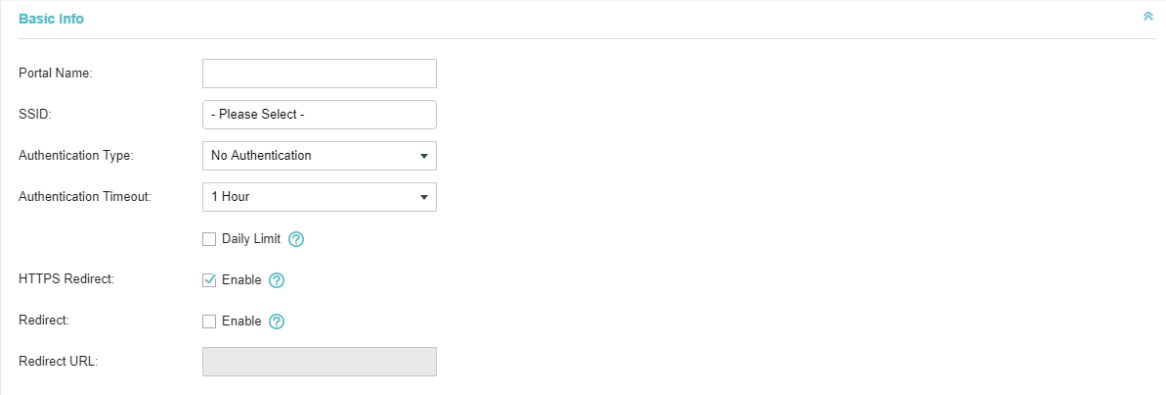
These authentication methods are available: No Authentication, Simple Password, Local User, Voucher, SMS, Facebook, External RADIUS Server and External Portal Server. The following sections introduce how to configure each Portal authentication.

3.1 No Authentication

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

Follow the steps below to configure No Authentication:

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

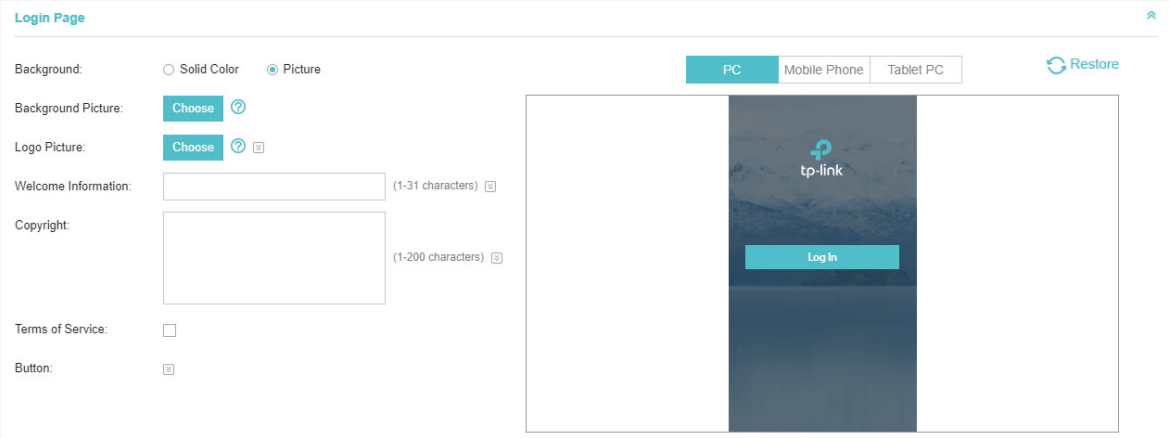


Configure the following parameters:

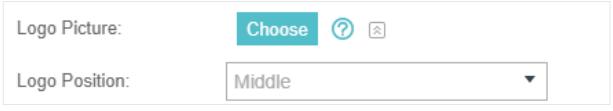
Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **No Authentication**.
Authentication Timeout	With Daily Limit disabled, the client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days** and **Custom**. **Custom** allows you to define the time in days, hours and minutes. The default value is one hour. With Daily Limit enabled, the client's authentication will expire after the time period you set and the client cannot log in again in the same day. Options include **30 Minutes, 1 Hour, 2 Hours, 4 Hours** and **Custom**. **Custom** allows you to define the time in hours and minutes. The default value is 30 minutes.
Daily Limit	With Daily Limit enabled, after authentication times out, the user cannot get authenticated again in the same day.

HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

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



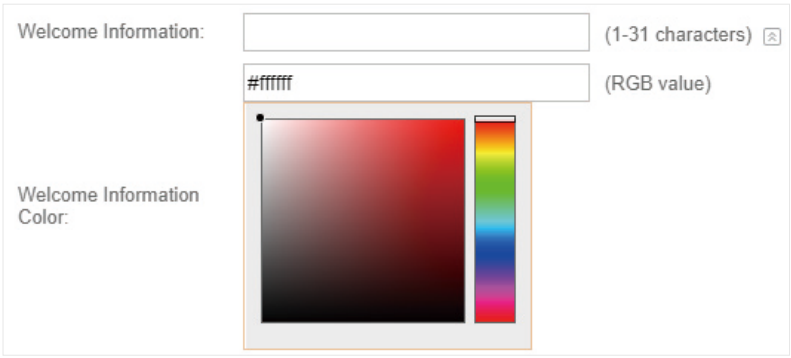
Configure the following parameters:

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

Welcome Information

Specify the welcome information.

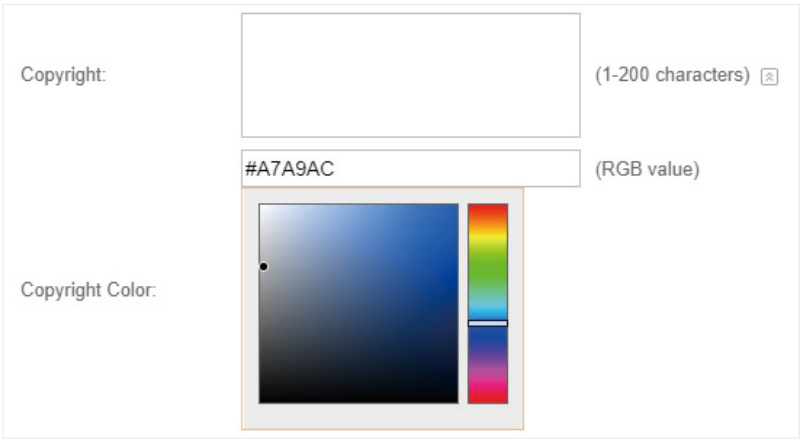
In addtion, you can click and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Copyright

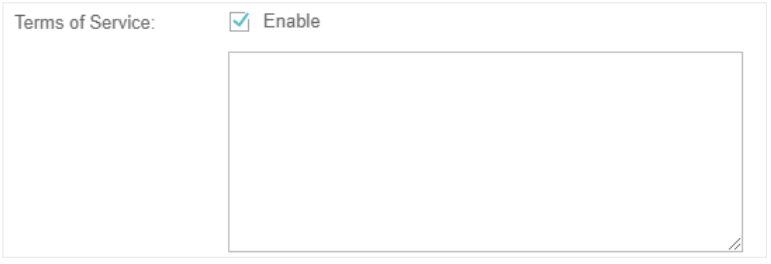
Specify the copyright information.

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

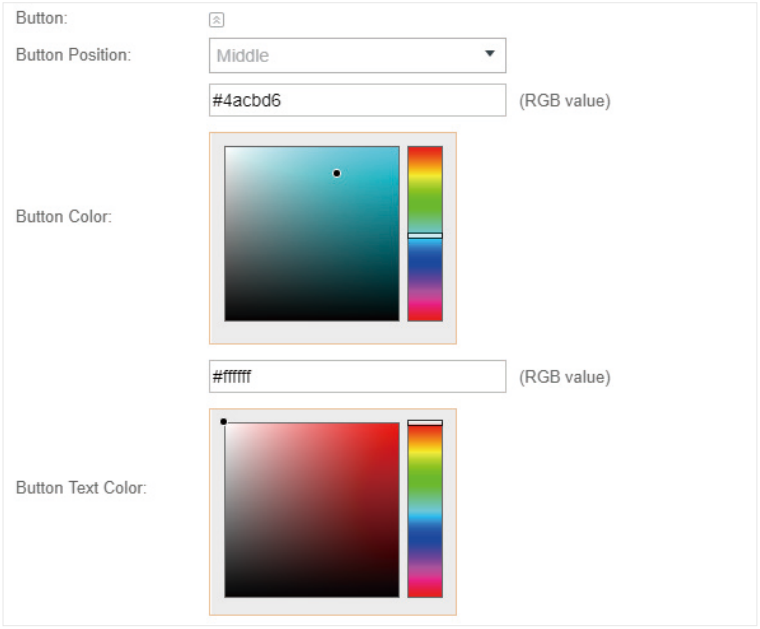


Terms of Service

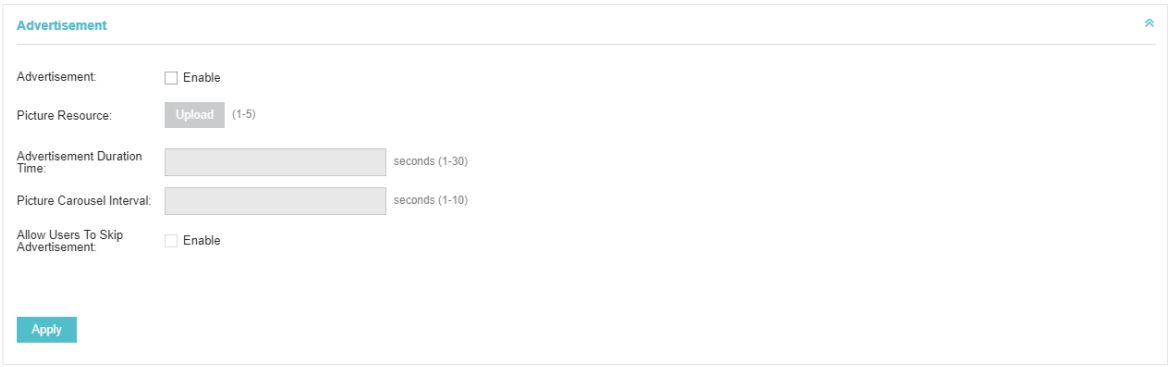
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.



Button	Click and configure the button. **Button Position**: Set the position of the login button. The options include **Middle, Upper** and **Lower.** **Button Color**: Select your desired login button color through the color picker or by entering the RGB value manually. **Button Text Color**: Select your desired text color for the button through the color picker or by entering the RGB value manually.



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



Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow Users To Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.

Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

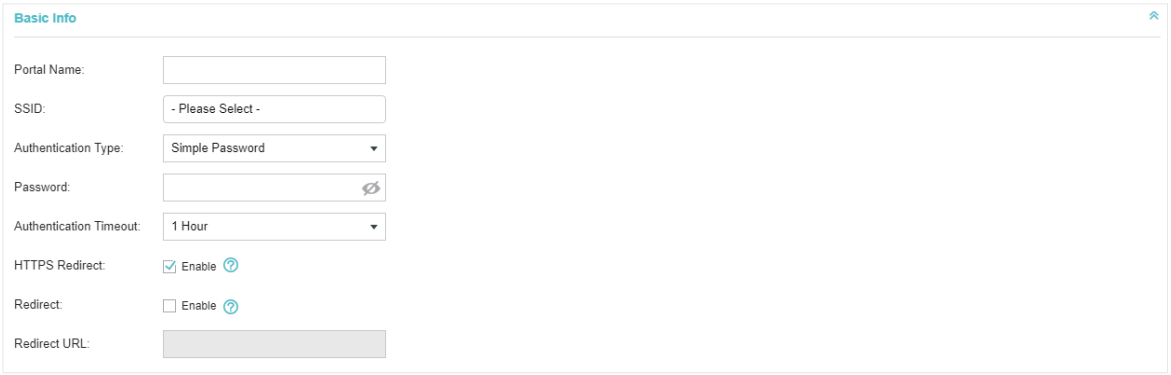
5. Click **Apply**.

3.2 Simple Password

With this Simple Password configured, clients are required to enter the correct password to pass the authentication.

Follow the steps below to configure No Simple Password Portal:

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

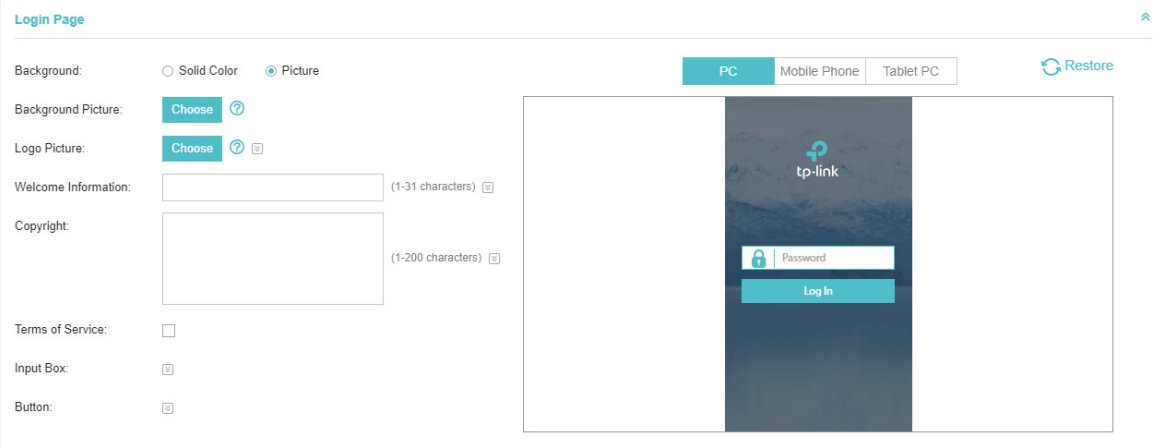


Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **Simple Password**.
Password	Set the password for authentication.

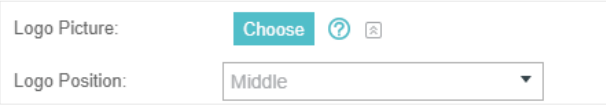
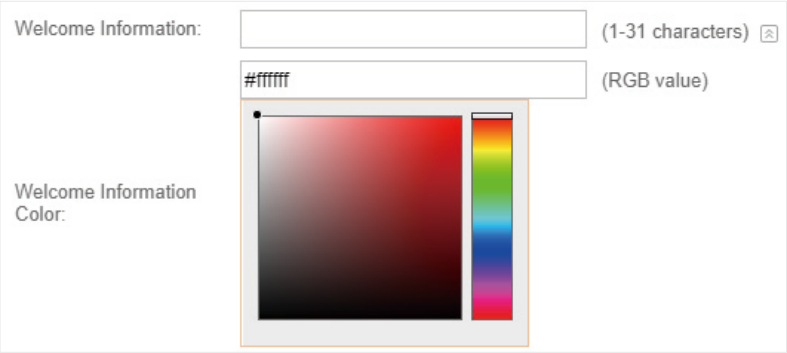
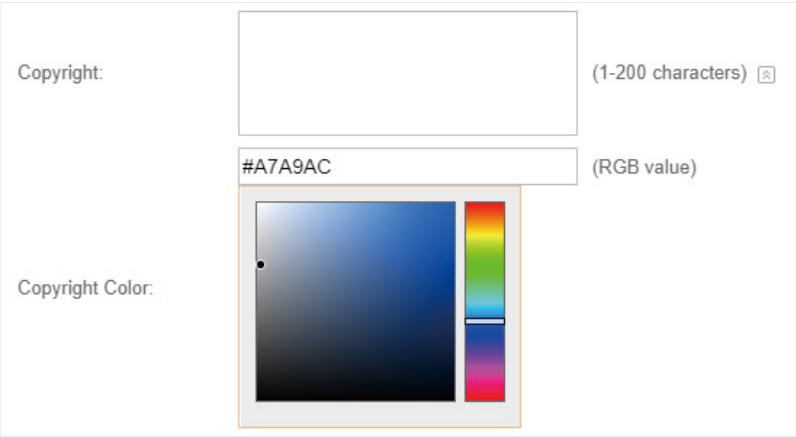
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days** and **Custom**. **Custom** allows you to define the time in days, hours and minutes. The default value is one hour.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

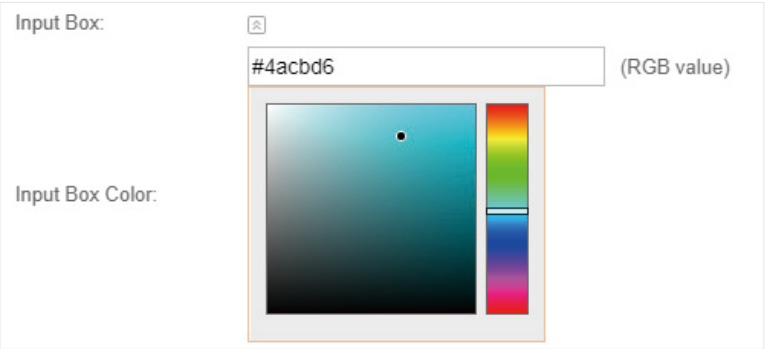
3. In the **Login Page** section, configure the login page for the Portal.



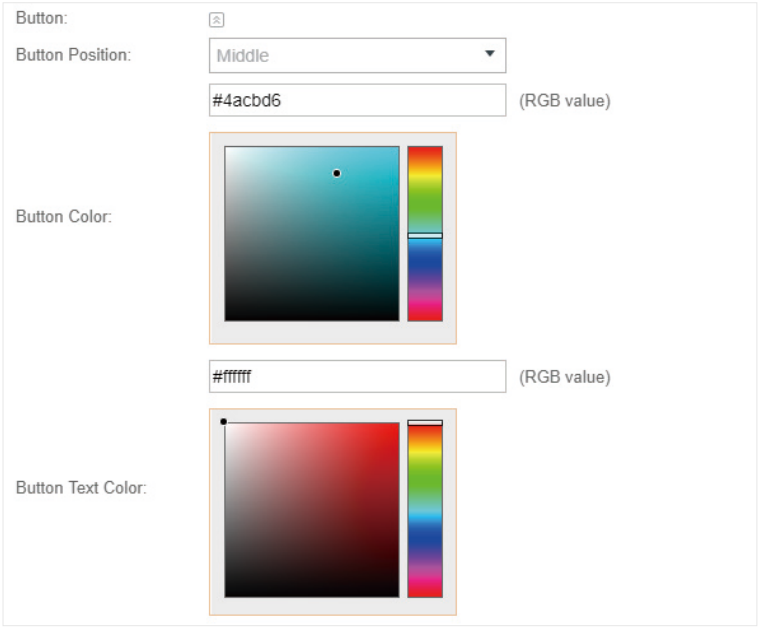
Configure the following parameters:

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

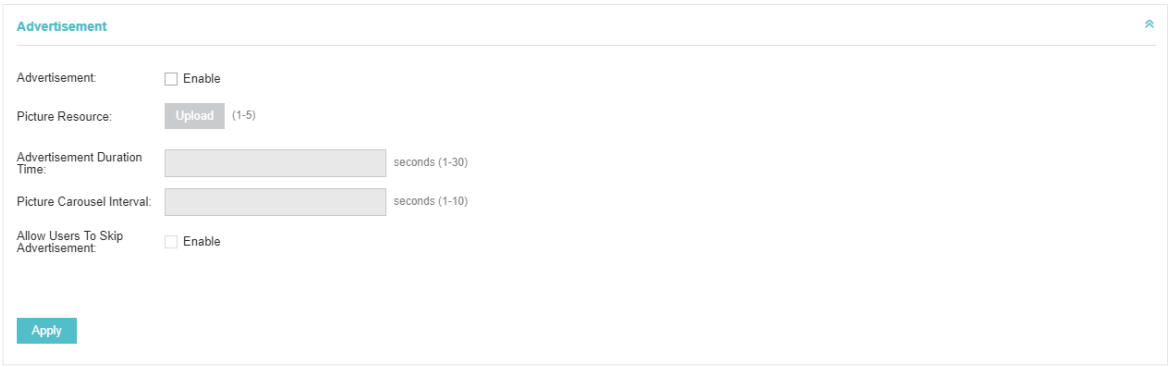
Logo Picture	Click the **Choose** button and select a picture from your PC. Drag and scale the clipping region to edit the picture and click **Confirm**. In addtion, you can click and configure the logo position. The options include **Middle, Upper** and **Lower**. 
Welcome Information	Specify the welcome information. In addtion, you can click and select your desired text color for the welcome information through the color picker or by entering the RGB value manually. 
Copyright	Specify the copyright information. In addtion, you can click and select your desired text color for Copyright information through the color picker or by entering the RGB value manually. 

Terms of Service	Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box. 
Input Box	Click and configure the input box. Select your desired color for the input box through the color picker or by entering the RGB value manually. 

Button	Click and configure the button. **Button Position**: Set the position of the login button. The options include **Middle, Upper** and **Lower.** **Button Color**: Select your desired login button color through the color picker or by entering the RGB value manually. **Button Text Color**: Select your desired text color for the button through the color picker or by entering the RGB value manually.



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



Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow Users To Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.

Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

5. Click **Apply**.

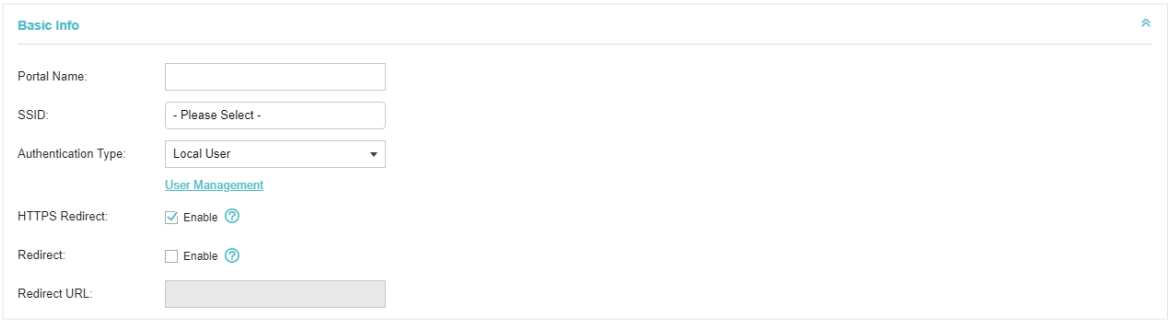
3.3 Local User

With this Local User configured, clients are required to enter the correct username and password of the login account to pass the authentication. You can create multiple accounts and assign different accounts for different users.

Configure Local User Portal

Follow the steps below to configure Local User Portal:

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

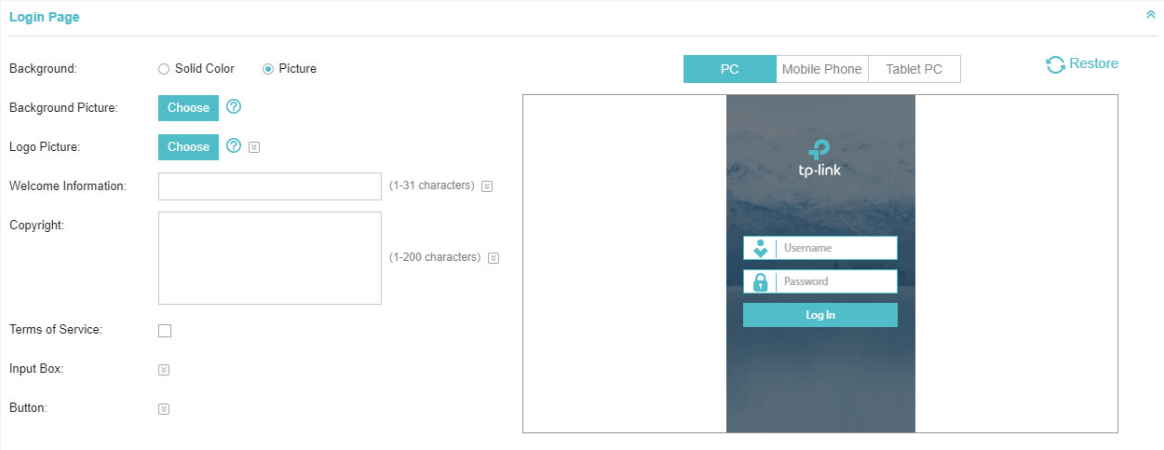


Configure the following parameters:

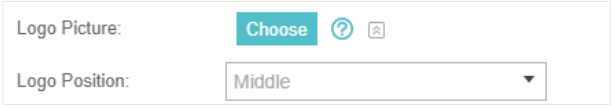
Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **Local User**.
User Management	You can click this button to configure user accounts for authentication later. Please refer to Create Local User Accounts.

HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

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



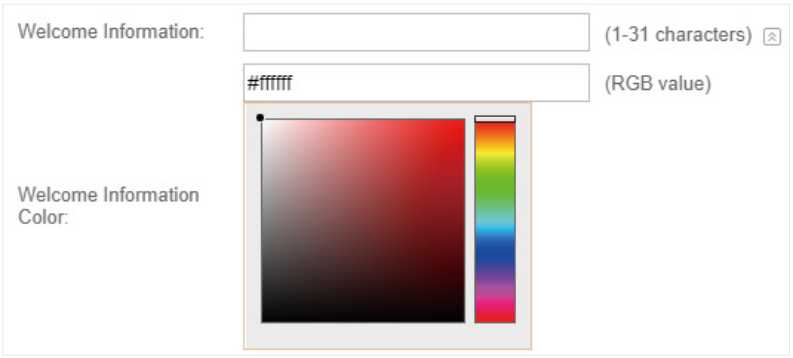
Configure the following parameters:

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

Welcome Information

Specify the welcome information.

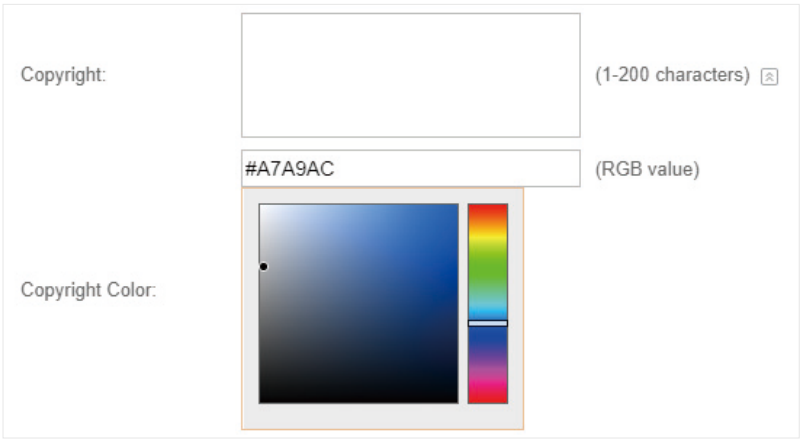
In addtion, you can click and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Copyright

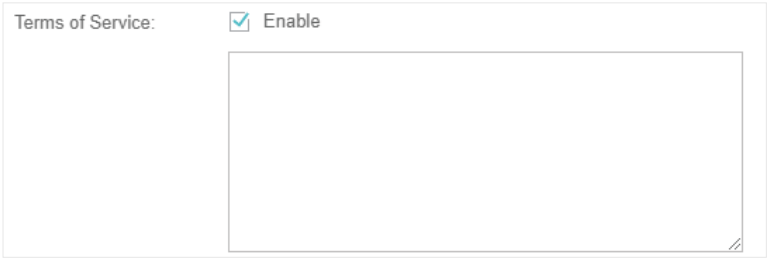
Specify the copyright information.

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



Terms of Service

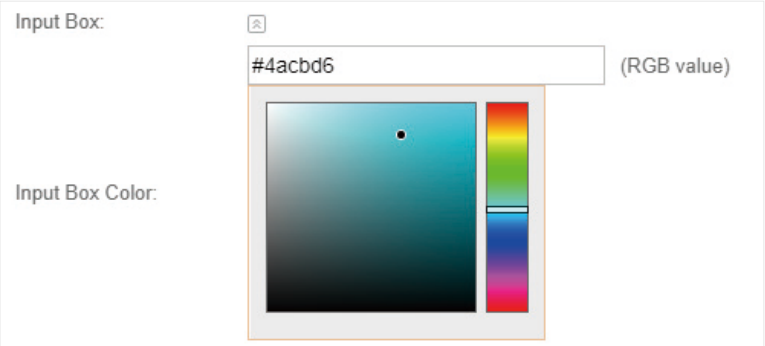
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.



Input Box

Click and configure the input box.

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



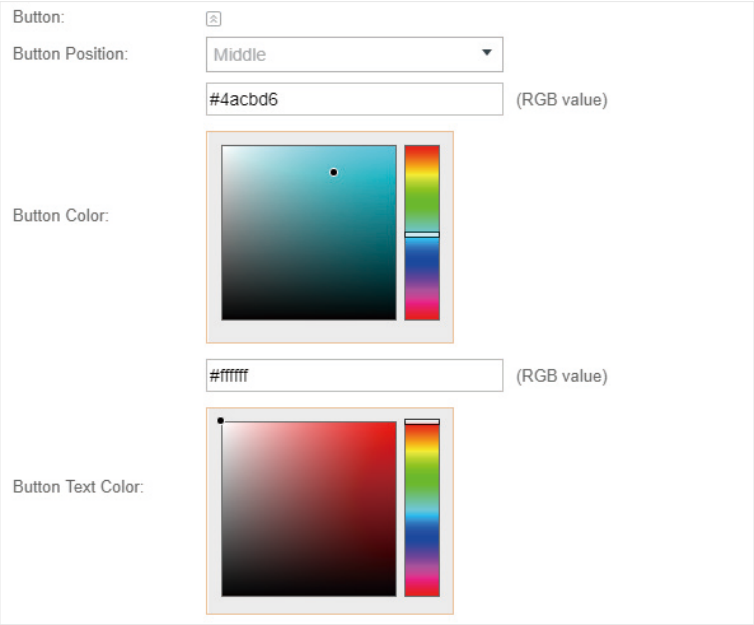
Button

Click and configure the button.

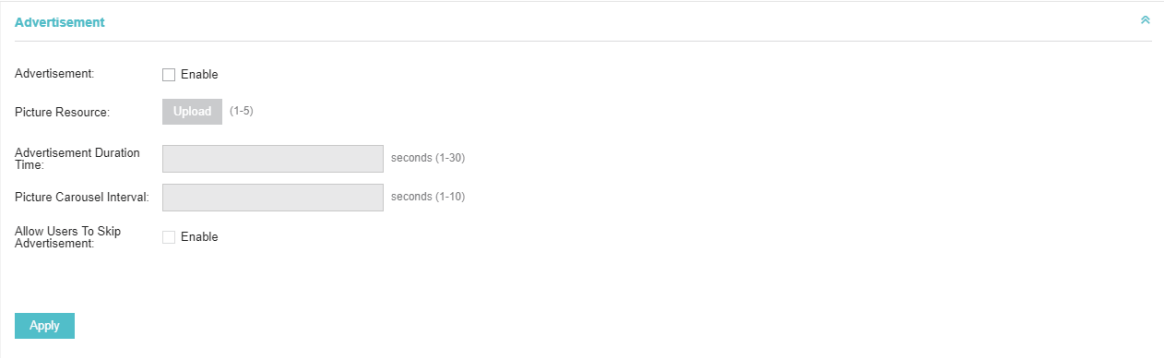
Button Position: Set the position of the login button. The options include **Middle, Upper** and **Lower.**

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

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



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



Configure the following parameters:

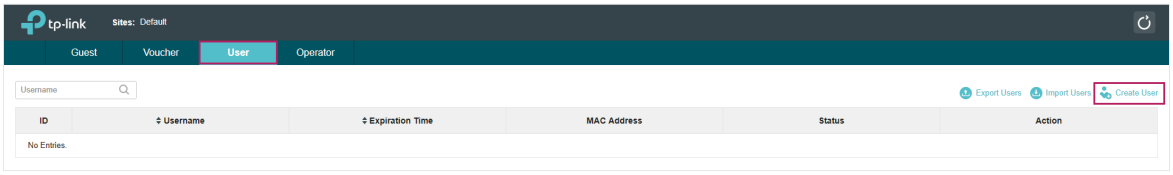
Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow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

5. Click **Apply**.

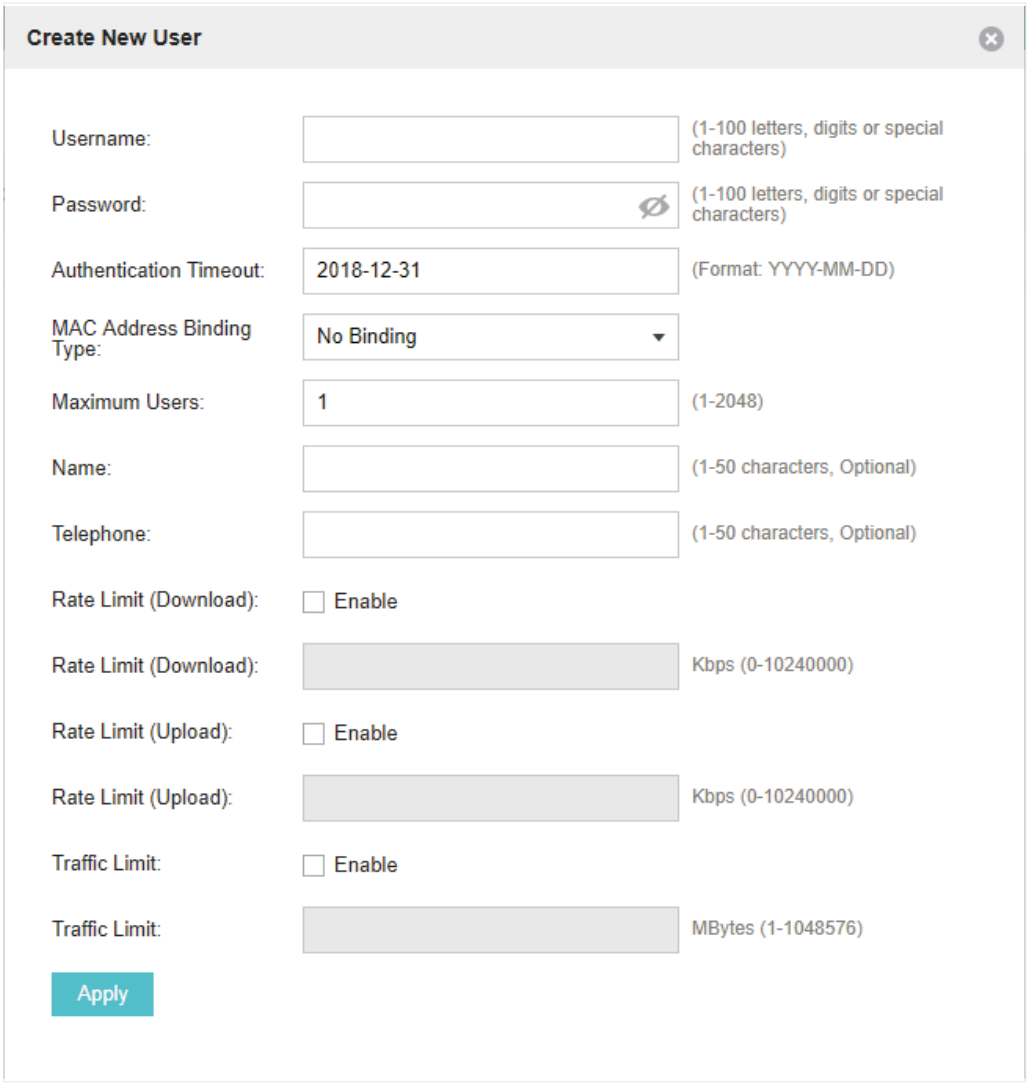
Create Local User Accounts

Follow the steps below to create the user accounts for authentication:

1. In the **Basic Info** section on the portal configuration page, click **User Management**. The management page will appear. Go to the **User** page and click Create User .



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



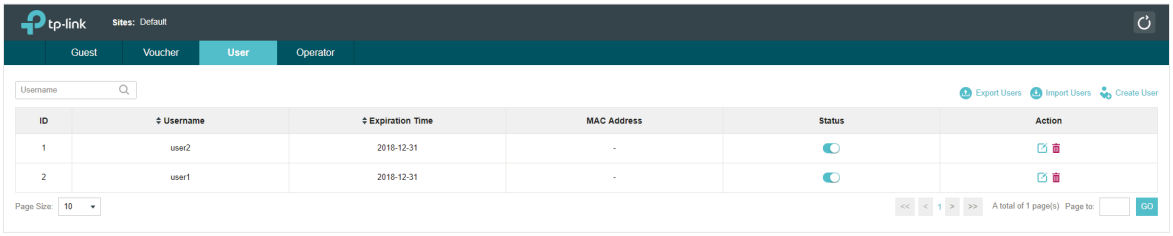
Configure the following parameters:

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

Maximum Users	Specify the maximum number of users able to use this account to pass the authencitation.
Name	Specify a name for identification.
Telephone	Specify a telephone number for identification.
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.
Traffic Limit	Select whether to enable traffic limit. With this option enabled, you can specify the total traffic limit for the user. Once the limit is reached, the user can no longer use this account to access the network.

3. In the same way, you can add more user accounts. The created user accounts will be displayed in the list. Users can use the username and password of the account to pass the portal authentication.

   By default, the account Status is , which means that the user account is enabled and valid. You can also click this button to disable the user account. The icon will be changed to , which means that the user account is disabled.



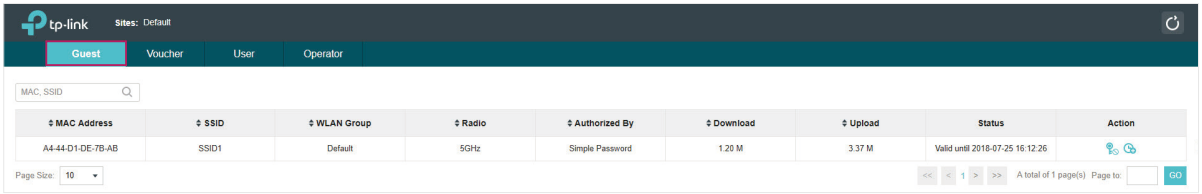
   Additionally, you can click Export Users to backup all the user account information into a CSV file or XLS file and save the file to your PC. If needed, you can click Import Users and select the file to import the account information to the list.

Note:

Using Excel to open the CSV file may cause some numerical format changes, and the number may be displayed incorrectly. If you use Excel to edit the CSV file, please set the cell format as text.

Manage the Guests

On the Guest page, you can view the information of clients that have passed the portal authentication and manage the clients.



You can select an icon to execute the corresponding operation:

	Disconnect client.
	Extend the effective time.

Create Operator Accounts

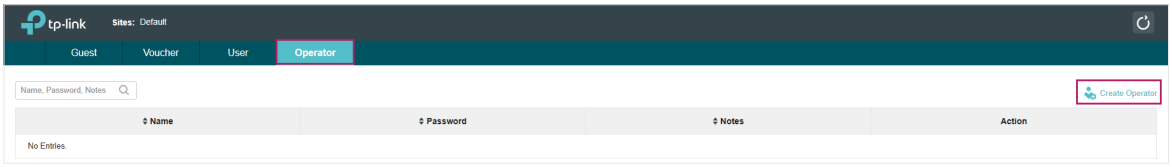
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://Omada Controller Host's IP Address:8043/hotspot** (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.

Note:

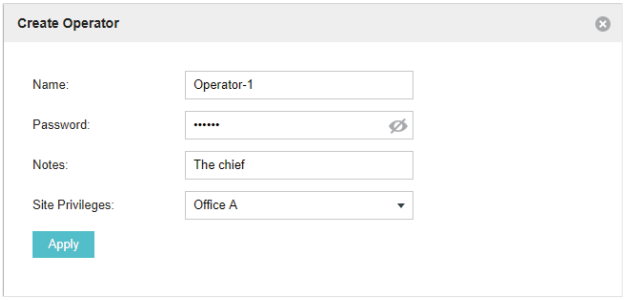
- Make sure the host that is used to enter the portal management page with operator account can visit the Controller host.
- Only the user that log in to the controller with the administrator role can add or remove the operator account for portal management.
- The users who enter the portal management page by operator account can only create local user accounts and vouchers and manage the clients.

Follow the steps below to create Operator account.

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



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



3. Specify the **Name**, **Password** and **Notes** of the Operator account.
4. Select **Site Privileges** from the drop-down list (multiple options available) for the Operator account.
5. Click **Apply** to create an Operator account. Then other users can use this account to enter the hotspot management page.

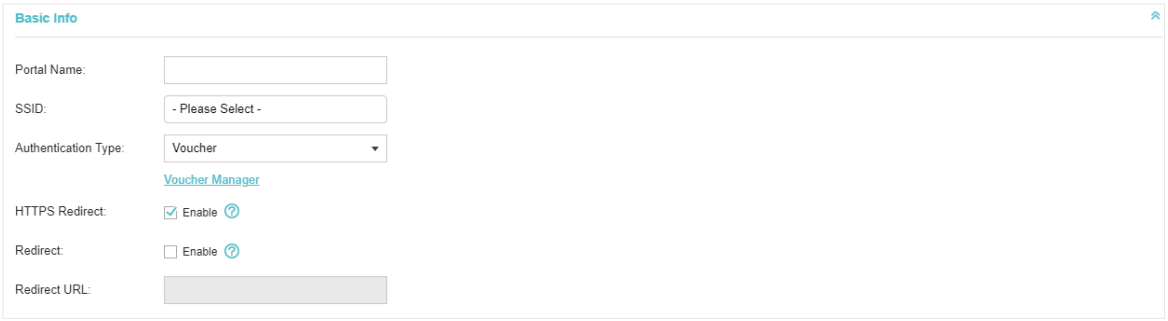
3.4 Voucher

With Voucher configured, you can distribute the vouchers automatically generated by the Omada Controller to the clients. Clients can use the vouchers to access the network.

Configure Voucher Portal

Follow the steps below to configure Voucher Portal:

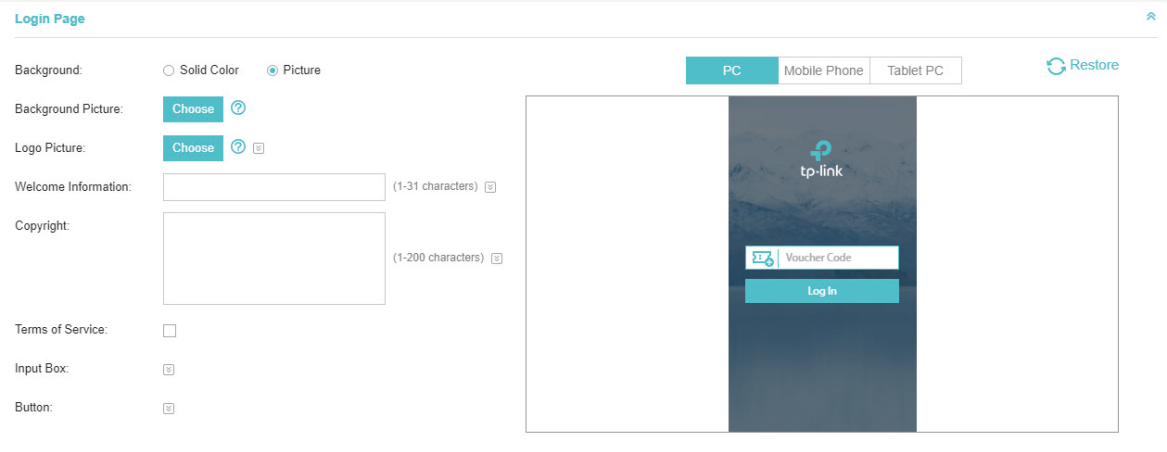
1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.
2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.



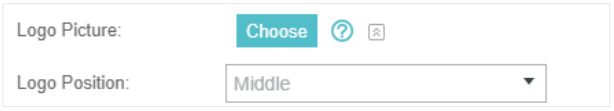
Configure the following parameters:

Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **Voucher**.
User Management	You can click this button to configure vouchers for authentication later. Please refer to Create Vouchers.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

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



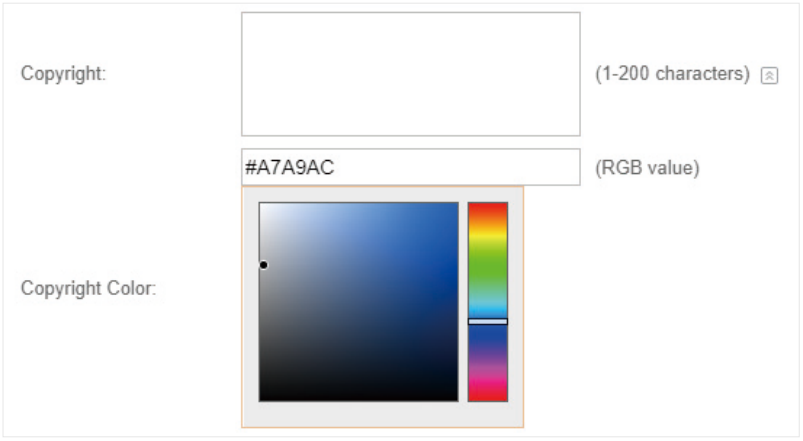
Configure the following parameters:

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

Copyright

Specify the copyright information.

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



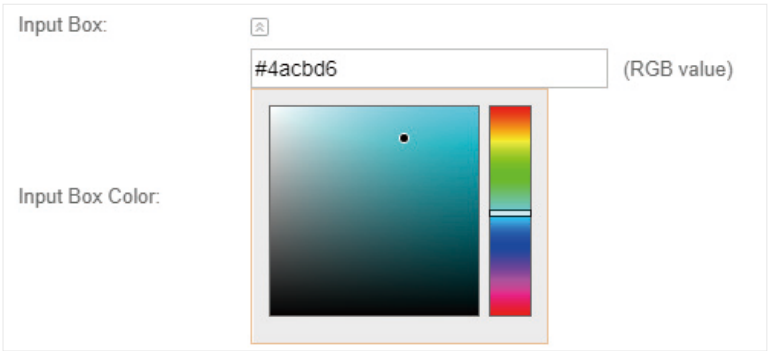
Terms of Service

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

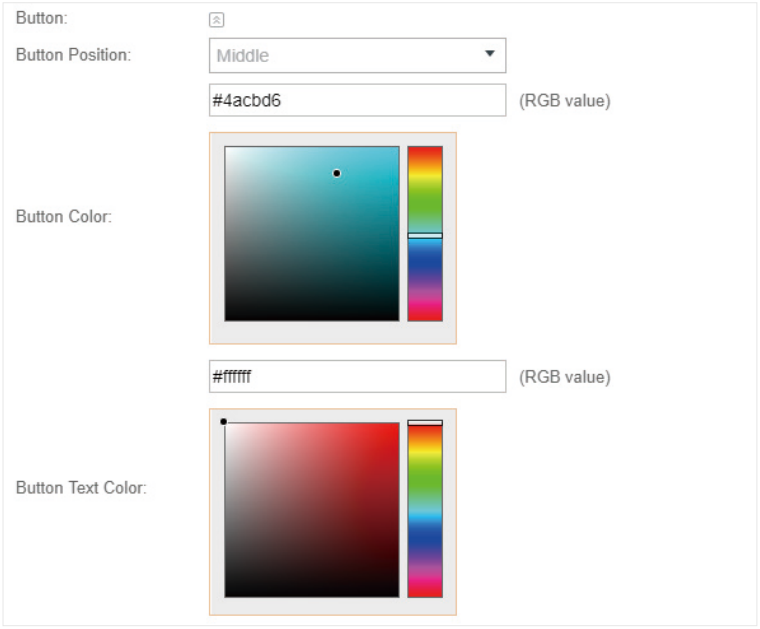
Input Box

Click and configure the input box.

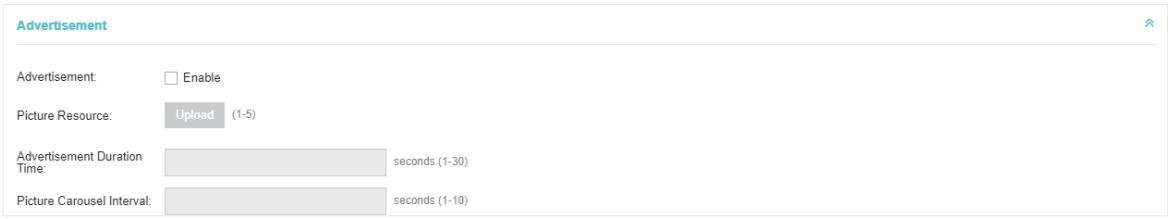
Select your desired color for the input box through the color picker or by entering the RGB value manually.



Button	Click and configure the button. **Button Position**: Set the position of the login button. The options include **Middle, Upper** and **Lower.** **Button Color**: Select your desired login button color through the color picker or by entering the RGB value manually. **Button Text Color**: Select your desired text color for the button through the color picker or by entering the RGB value manually.



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



Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow Users To Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.

Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

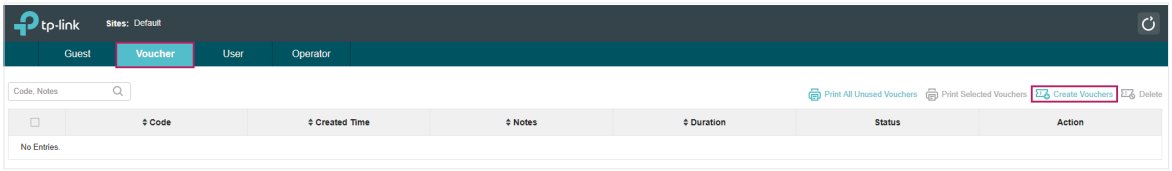
5. Click **Apply**.

Create Vouchers

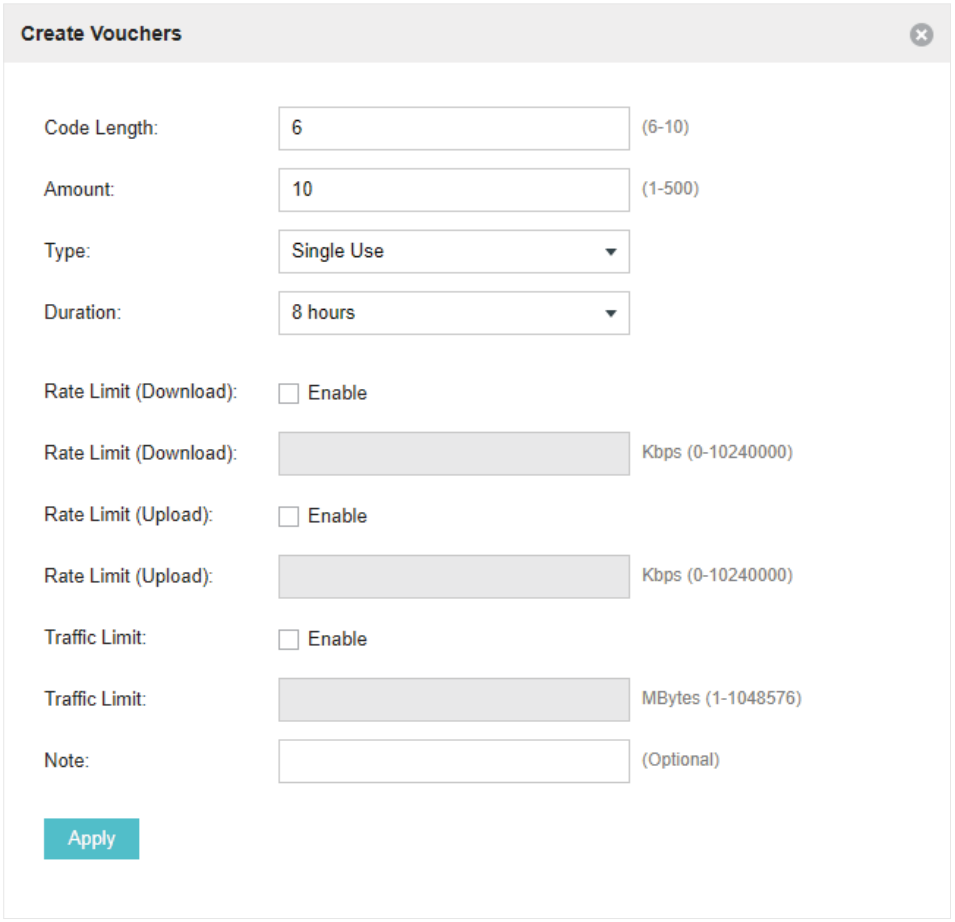
Follow the steps below to create vouchers for authentication:

1. In the **Basic Info** section, click **Voucher Manager**. The voucher management page will appear.

   Go to the **Voucher** page and click Create Vouchers .



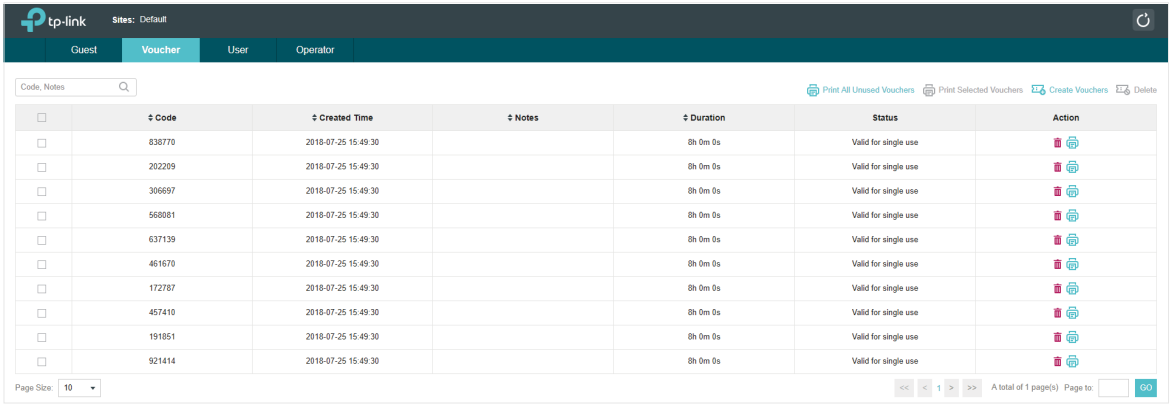
2. The following window will pop up. Configure the required parameters and click **Apply**.



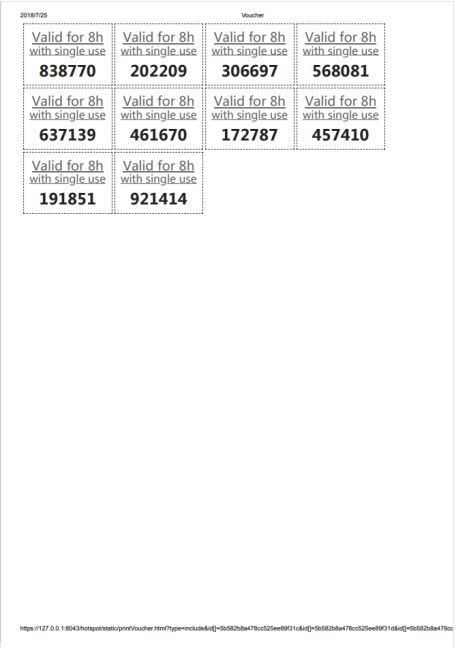
Configure the following parameters:

Code Length	Specify the length of the voucher codes to be created.
Amount	Enter the voucher amount to be generated.
Type	Select **Single Use** or **Multi Use**. Single Use means one voucher can only be distributed to one client. Multi Use means one voucher can be distributed to several clients, who can use the same voucher to access the network at the same time. If you select Multi Use, enter the value of **Max Users**. When the number of clients who are connected to the network with the same voucher reaches the value, no more clients can use this voucher to access the network.
Duration	Select the period of validity of the Voucher. The options include **8 hours**, **2 days** and **User-defined**. The period of valid of the voucher is reckoned from the time when it is used for the first time.
Rate Limit (Download)	Select whether to enable download rate limit. With this option enabled, you can specify the limit of download rate.
Rate Limit (Upload)	Select whether to enable upload rate limit. With this option enabled, you can specify the limit of upload rate.
Traffic Limit	Specify the total traffic limit for one voucher. Once the limit is reached, the client can no longer access the network using the voucher.
Notes	Enter a description for the Voucher (optional).

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



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

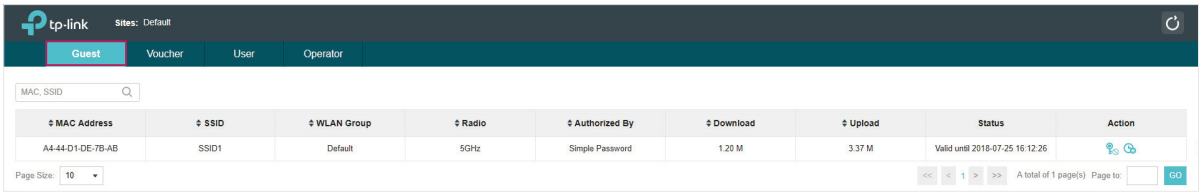


5. Distribute the vouchers to clients, and then they can use the codes to pass authentication.

6. When the vouchers are invalid, you can click to delete the Voucher or click Delete to delete the selected vouchers.

Manage the Guests

On the Guest page, you can view the information of clients that have passed the portal authentication and manage the clients.



You can select an icon to execute the corresponding operation:

	Restrict the client to access the network.
	Extend the effective time.

Create Operator Accounts

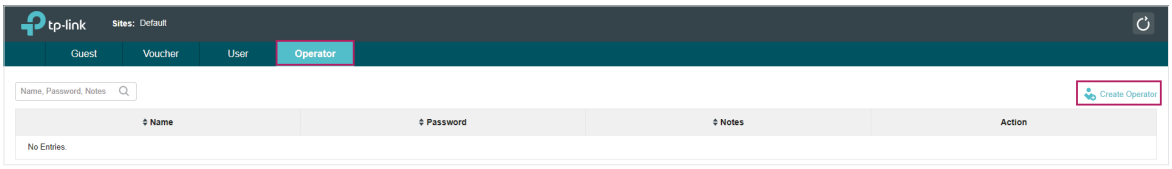
Operator account can be used to remotely manage the Local User Portal and Voucher Portal. Other users can visit the URL **https://Omada Controller Host's IP Address:8043/hotspot** (For example: https://192.168.0.64:8043/hotspot) and use the Operator account to enter the portal management page.

Note:

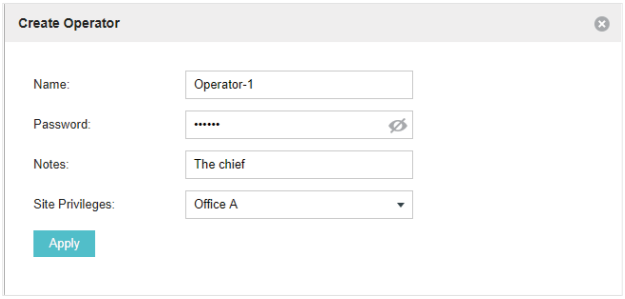
- Make sure the host that is used to enter the portal management page with operator account can visit the Controller host.
- Only the user that log in to the controller with the administrator role can add or remove the operator account for portal management.
- The users who enter the portal management page by operator account can only create local user accounts and vouchers and manage the clients.

Follow the steps below to create Operator account.

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



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



3. Specify the **Name**, **Password** and **Notes** of the Operator account.
4. Select **Site Privileges** from the drop-down list (multiple options available) for the Operator account.
5. Click **Apply** to create an Operator account. Then other users can use this account to enter the hotspot administrative system.

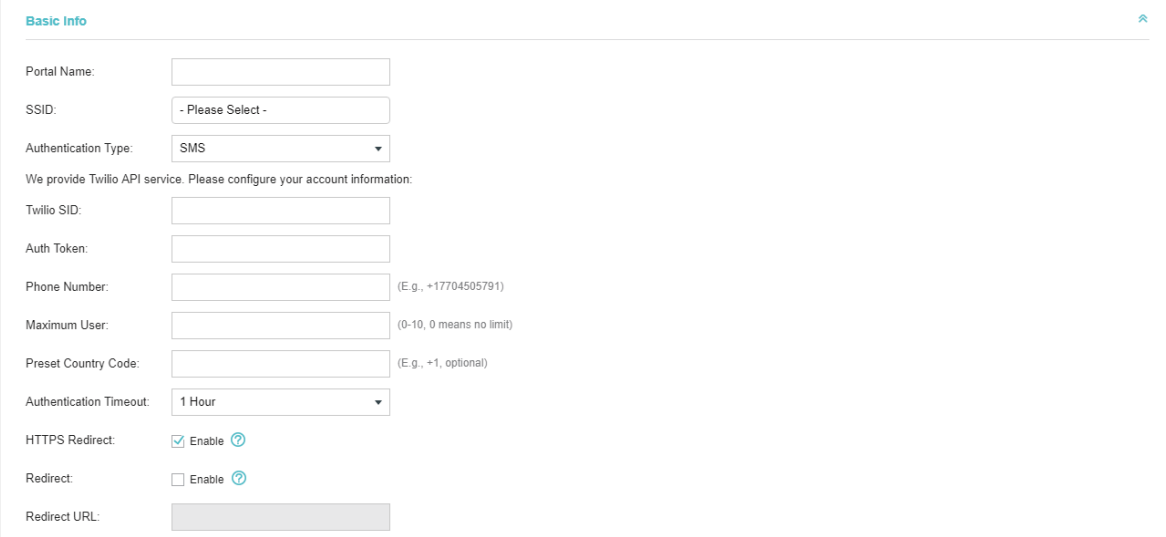
3.5 SMS

With SMS portal configured, client can get verification codes using their mobile phones and enter the received codes to pass the authentication.

Follow the steps below to configure SMS Portal:

1. Go to www.twilio.com/try-twilio and get a Twilio account. Buy the Twilio service for SMS. Then get the account information, including ACCOUNT SID, AUTH TOKEN and Phone number.
2. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

3. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

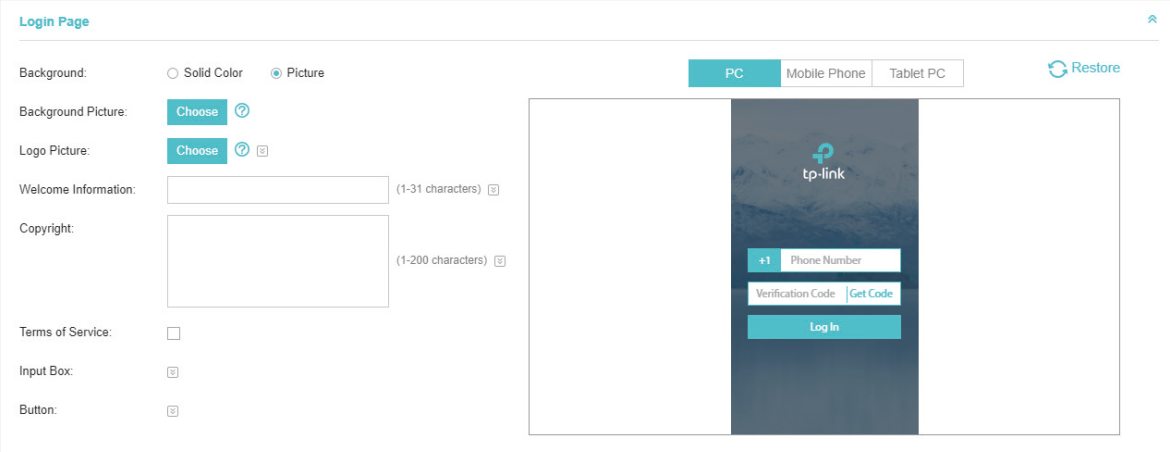


Configure the following parameters:

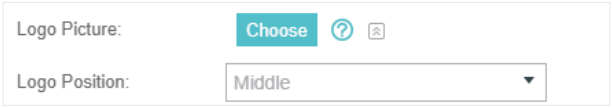
Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **SMS**.
Twilio SID	Enter the Account SID for Twilio API Credentials.
Auth Token	Enter the Authentication Token for Twilio API Credentials.
Phone Number	Enter the phone number that is used to send verification messages to the clients.
Maximum Users	A telephone can get several codes via messages one by one, and different clients can use different codes to pass the authentication. However, the number of clients that is allowed to be authenticated using the same telephone at the same time has a upper limit. Specify the upper limit in this field.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network. Options include **1 Hour, 8 Hours, 24 Hours, 7 Days** and **Custom**. **Custom** allows you to define the time in days, hours and minutes. The default value is one hour.
Preset Country Code	Set the default country code that will be filled automatically on the authentication page.

HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

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



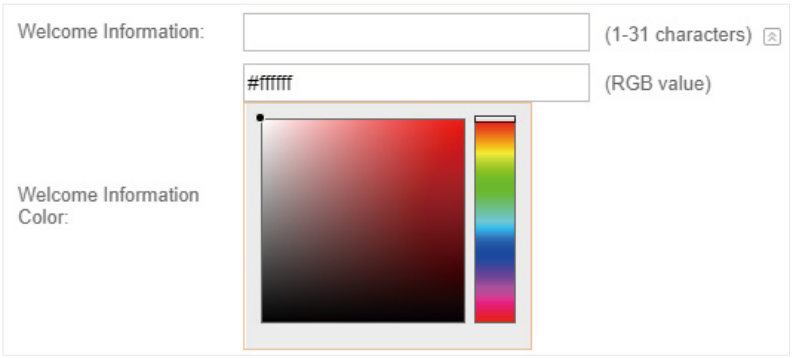
Configure the following parameters:

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

Welcome Information

Specify the welcome information.

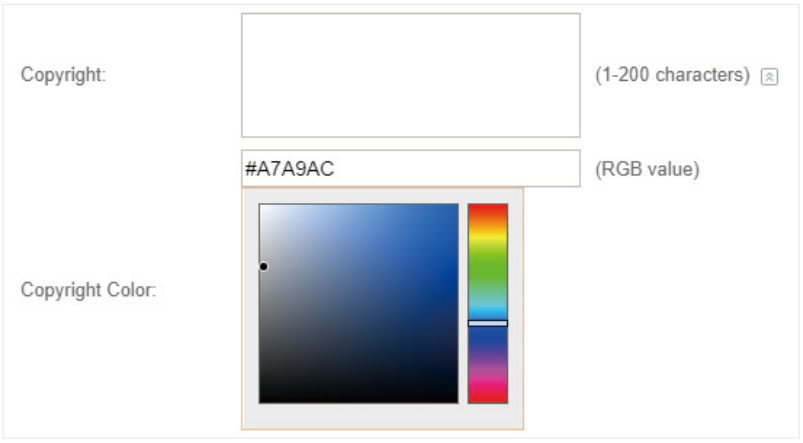
In addtion, you can click and select your desired text color for the welcome information through the color picker or by entering the RGB value manually.



Copyright

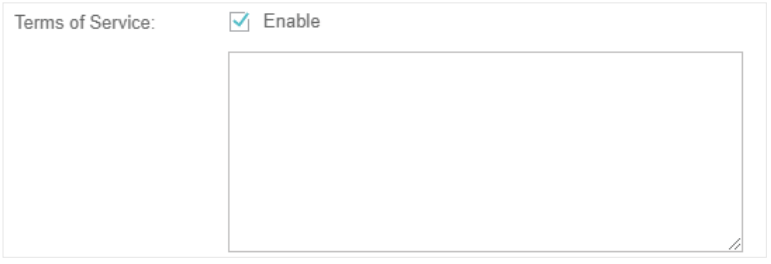
Specify the copyright information.

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



Terms of Service

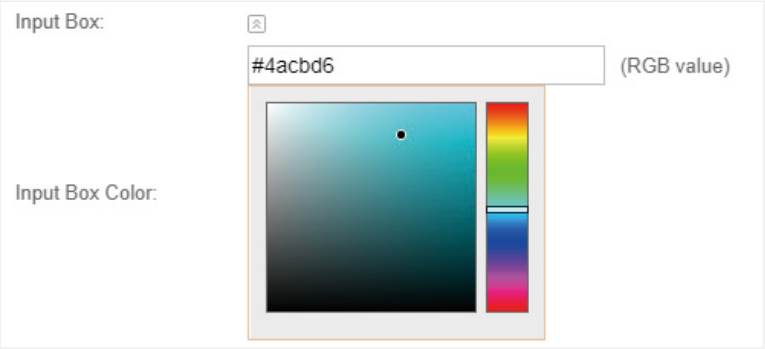
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.



Input Box

Click and configure the input box.

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



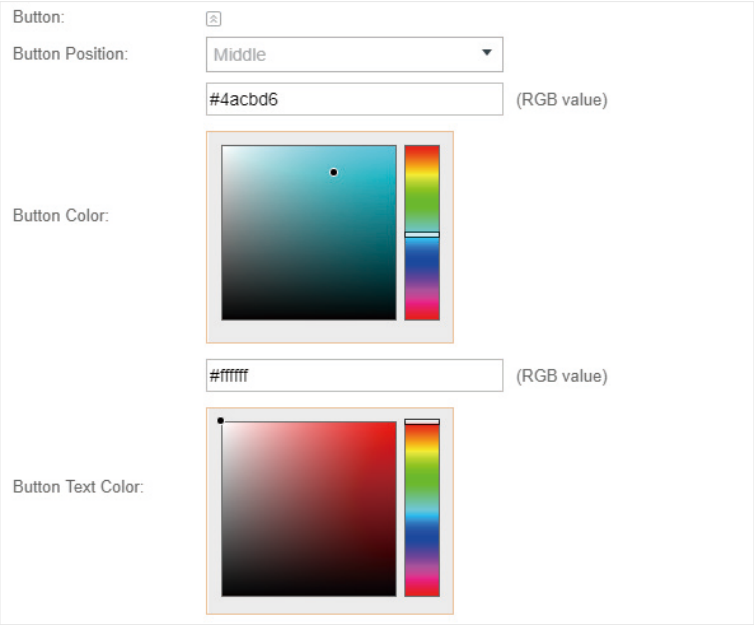
Button

Click and configure the button.

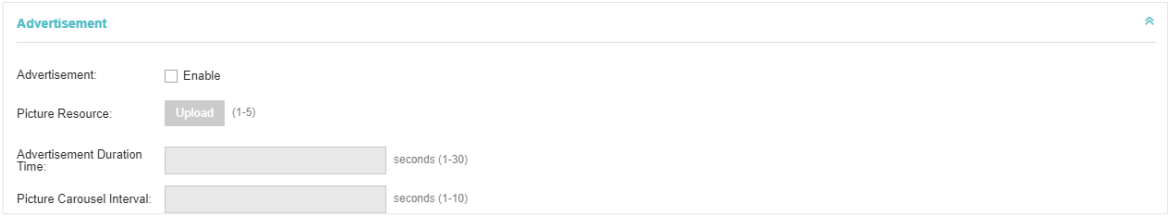
Button Position: Set the position of the login button. The options include **Middle, Upper** and **Lower.**

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

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



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



Configure the following parameters:

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

6. Click **Apply**.

For more details about how to configure SMS Portal, refer to the configuration guide for SMS Portal.

3.6 Facebook

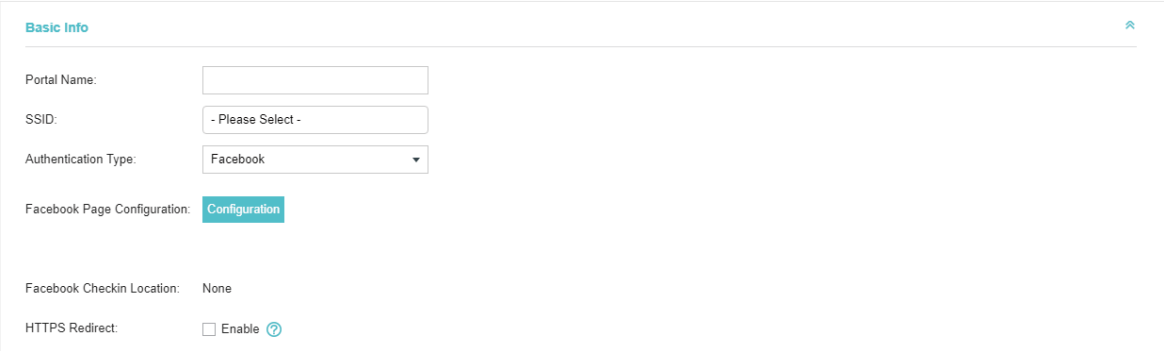
With Facebook Portal configured, when clients connect to your Wi-Fi, they will be redirected to your Facebook page. To access the internet, clients need to pass the authentication on the page.

Note:

Omada Controller will automatically create Free Authentication Policy entries for the Facebook Portal. You don't need to create them manually.

Follow the steps below to configure Facebook Portal:

1. Go to Facebook and get a Facebook account. Create your Facebook page according to your needs.
2. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.
3. Go back to the Portal configuration page. In the **Basic Info** section, complete the settings for the portal authentication.



Configure the following parameters:

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

For more details about how to configure Facebook Portal, refer to the configuration guide for Facebook Portal.

3.7 External RADIUS Server

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

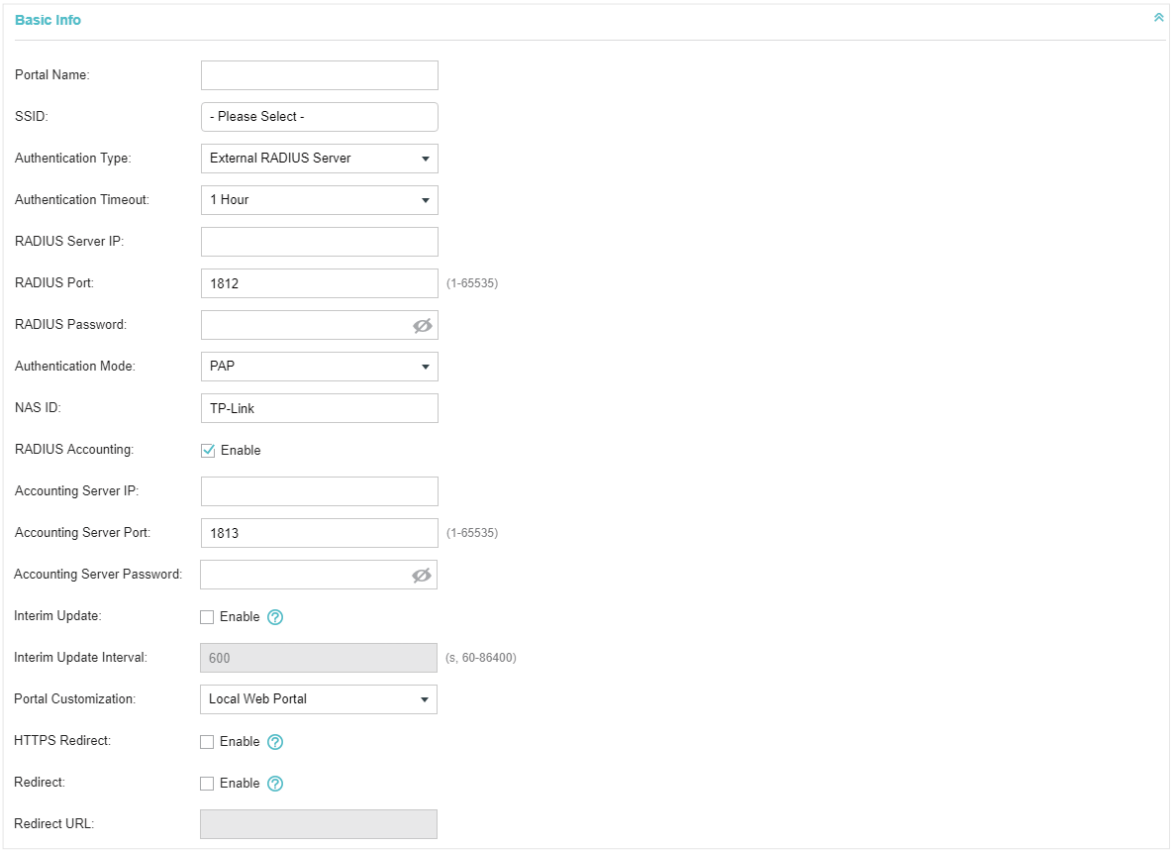
Note:

Omada Controller will automatically create Free Authentication Policy entries for the External RADIUS Portal.

Follow the steps below to configure External RADIUS Server Portal:

1. Go to **Wireless Settings > Basic Wireless Settings** and create an SSID for the Portal.

2. Go back to the Portal configuration page. In the **Basic Info** section, complete the basic settings for the portal authentication.

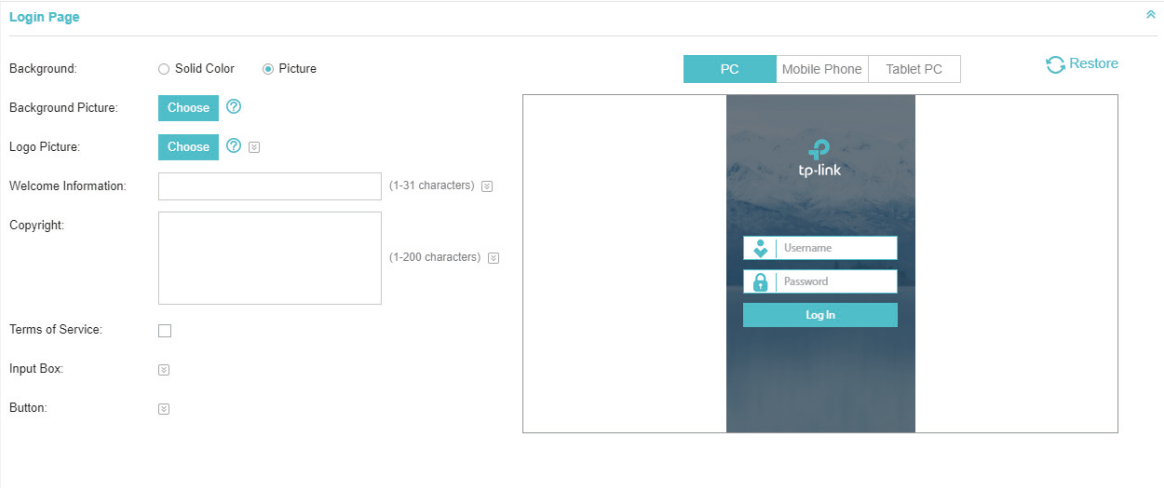


Configure the following parameters:

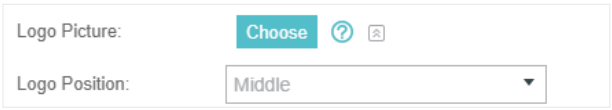
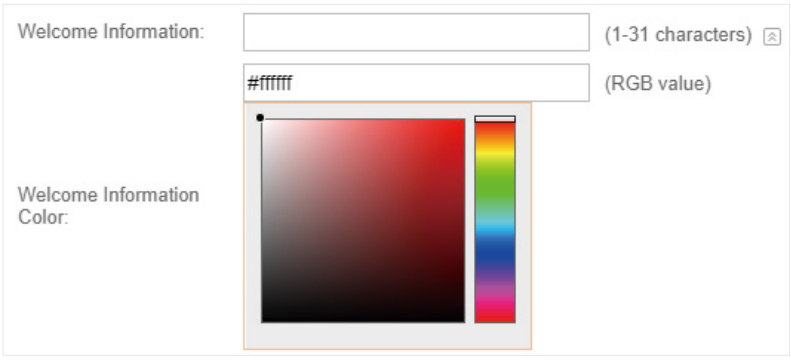
Portal Name	Specify a name for the Portal.
SSID	Select an SSID for the Portal.
Authentication Type	Select **External RADIUS Server**.
Authentication Timeout	The client's authentication will expire after the time period you set and the client needs to log in again on the web authentication page to access the network. Options incIde **1 Hour, 8 Hours, 24 Hours, 7 Days, Custom**. **Custom** allows you to define the time in days, hours, and minutes. The default value is one hour.
RADIUS Server IP	Enter the IP address of the RADIUS server.
RADIUS Port	Enter the port number you have set on the RADIUS server.
RADIUS Password	Enter the password you have set on the RADIUS server.
Authentication Mode	Select the authentication protocol for the RADIUS server. Two authentication protocols are available: **PAP** and **CHAP**.

NAS ID	Configure a Network Access Server Identifier (NAS ID) using 1 to 64 characters on the portal. The NAS ID is sent to the RADIUS server by the controller through an authentication request packet. With the NAS ID which classifies users to different groups, the RADIUS server can send a customized authentication response. The default value is **TP-Link**.
RADIUS Accounting	Enable or disable RADIUS Accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server. The default port number is 1813.
Accounting Server Password	Enter the shared secret key of the accounting server.
Interim Update	With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled. Enter the appropriate duration between updates for EAPs in **Interim Update Interval**.
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for EAPs. The default duration is 600 seconds.
Portal Customization	Select Local Web Portal or External Web Portal. **Local Web Portal**: If this option is selected, refer to step 3 to configure the login page and step 4 to configure the advertisement. **External Web Portal**: If this option is selected, follow the steps below. 1. Configure the external RADIUS server. 2. Enter the authentication login page's URL provided by the external portal server in the External Web Portal URL field. Note that you should update the External Web Portal after you upgrade your controller with old version to version 3.1.4 or above. Otherwise, the External Web Portal will not take effect.
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.
Redirect	If you enable this function, the portal will redirect the newly authenticated clients to the configured URL. It is disabled by default.
Redirect URL	If the Redirect function above is enabled, enter the URL that a newly authenticated client will be redirected to.

3. **Local Web Portal** is configured, configure the login page for the Portal in the **Login Page** section.



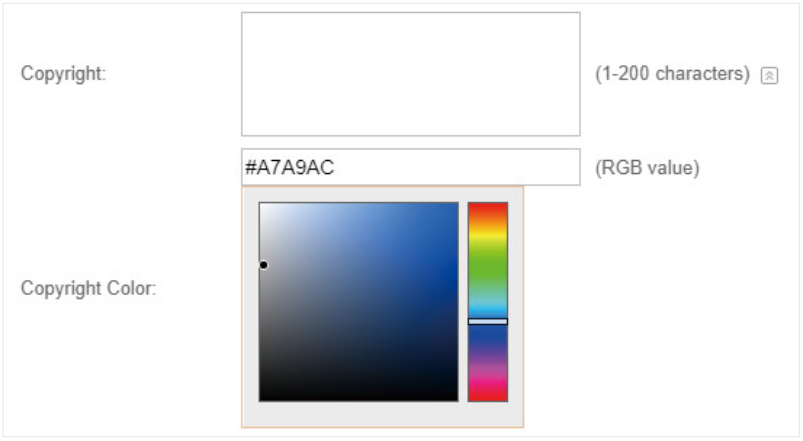
Configure the following parameters:

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

Copyright

Specify the copyright information.

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



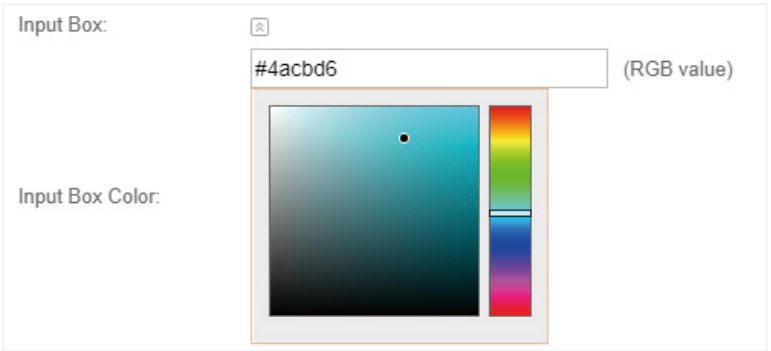
Terms of Service

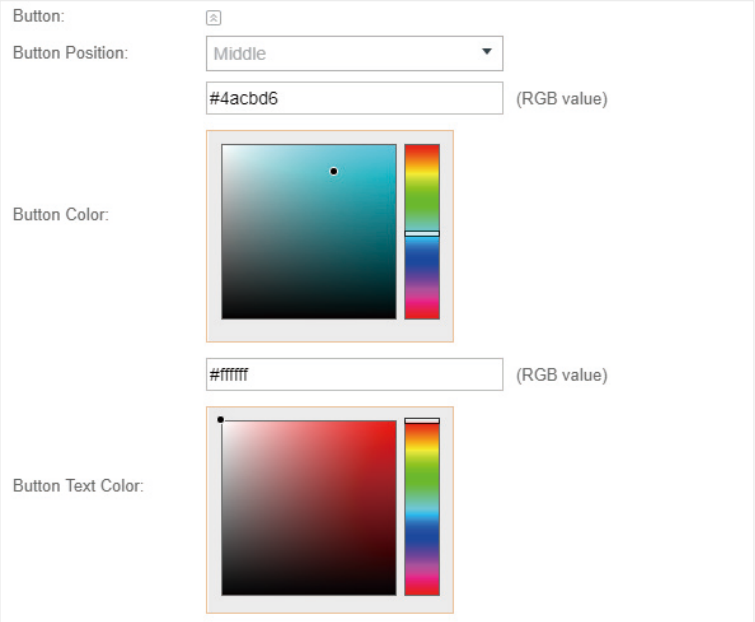
Enable or disable Terms of Service. With this option enabled, specify the terms of service in the following box.

Input Box

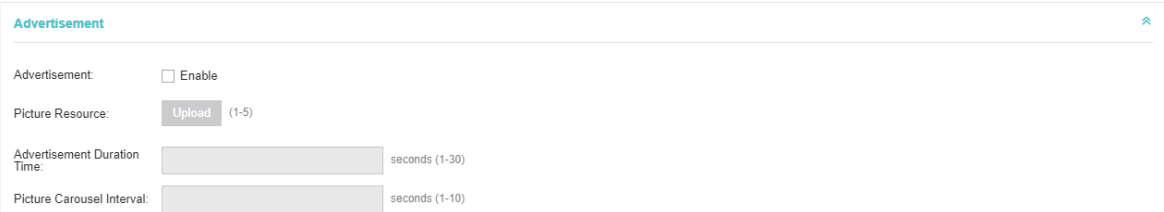
Click and configure the input box.

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



Button	Click and configure the button. **Button Position**: Set the position of the login button. The options include **Middle, Upper** and **Lower.** **Button Color**: Select your desired login button color through the color picker or by entering the RGB value manually. **Button Text Color**: Select your desired text color for the button through the color picker or by entering the RGB value manually. 

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



Configure the following parameters:

Advertisement	Specify whether to enable the Advertisement feature. With this feature enabled, you can add advertisement pictures on the authentication page. These advertisement pictures will be displayed before the login page appears. You can also allow users to skip the advertisement by enabling **Allow Users To Skip Advertisement**. The advertisement picture should be less than 2MB. And only JPG, PNG, BMP, GIF and JPEG file types are supported.
Picture Resource	Upload advertisement pictures. When several pictures are added, they will be played in a loop.

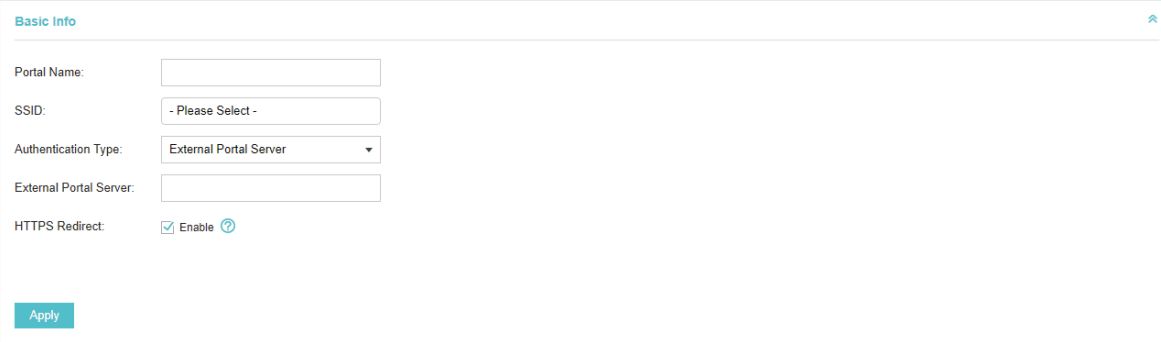
Advertisement Duration Time	Specify how long the advertisement will be displayed for. For this duration, the pictures will be played in a loop. If the duration time is not enough for all the pictures, the rest will not be displayed.
Picture Carousel Interval	Specify the picture carousel interval. For example, if this value is set as 5 seconds, the first picture will be displayed for 5 seconds, followed by the second picture for 5 seconds, and so on.
Allow Users To Skip Advertisement	Specify whether to enable this feature. With this feature enabled, the user can click the **Skip** button to skip the advertisement.

5. Click **Apply**.

3.8 External Portal Server

The option of External Portal Server is designed for the developers. They can customized their own authentication type according to the interface provided by Omada Controller, e.g. message authentication and WeChat authentication etc.

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



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

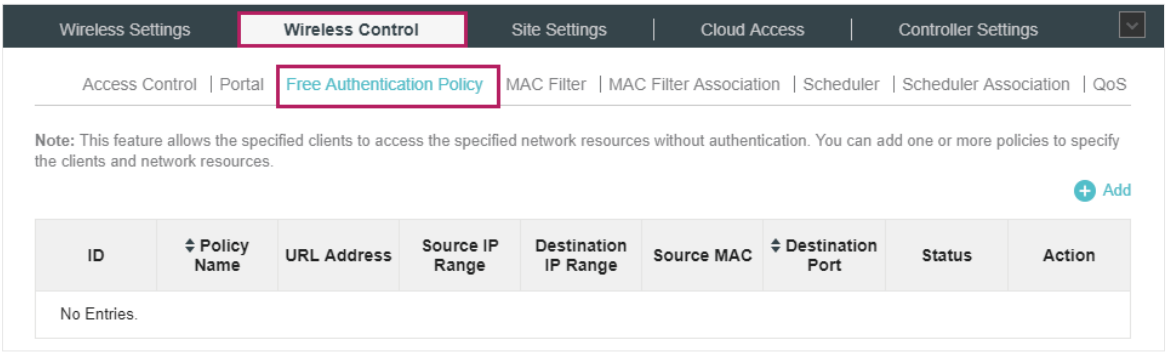
HTTPS Redirect	With this function enabled, the unauthorized clients will be redirected to the Portal page when they are trying to browse HTTPS websites. With this function disabled, the unauthorized clients cannot browse HTTPS websites and are not redirected to the Portal page.

3. Click **Apply**.

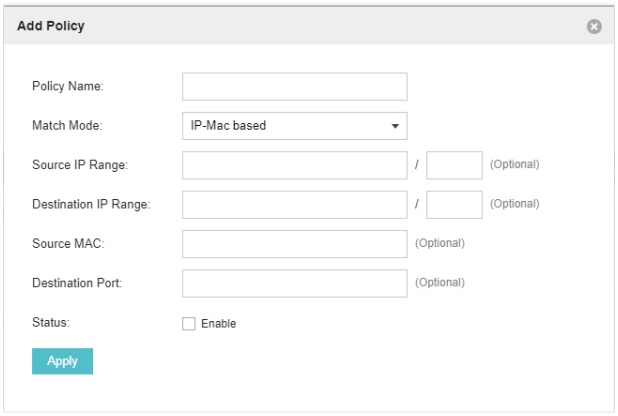
4 Free Authentication Policy

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

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



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



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

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

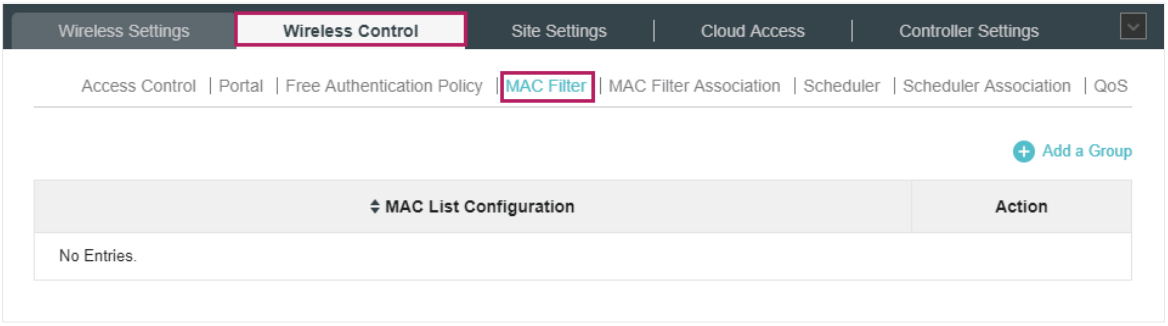
4. Click **Apply** and the policy is successfully added.

5 MAC Filter

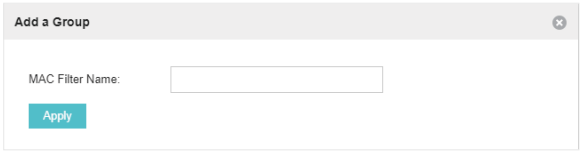
MAC filter can be used to allow or block the listed clients to access the network. Thereby it can effectively control the client's access to the wireless network.

Follow the steps below to configure MAC Filter.

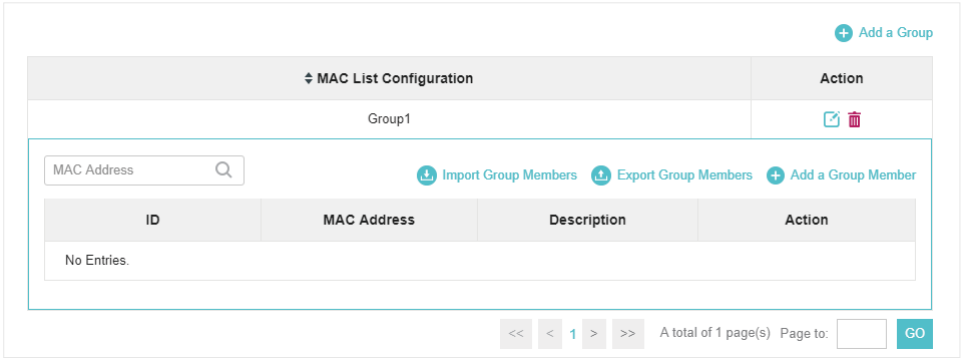
1. Go to **Wireless Control > MAC Filter** to add MAC Filter group and group members.



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

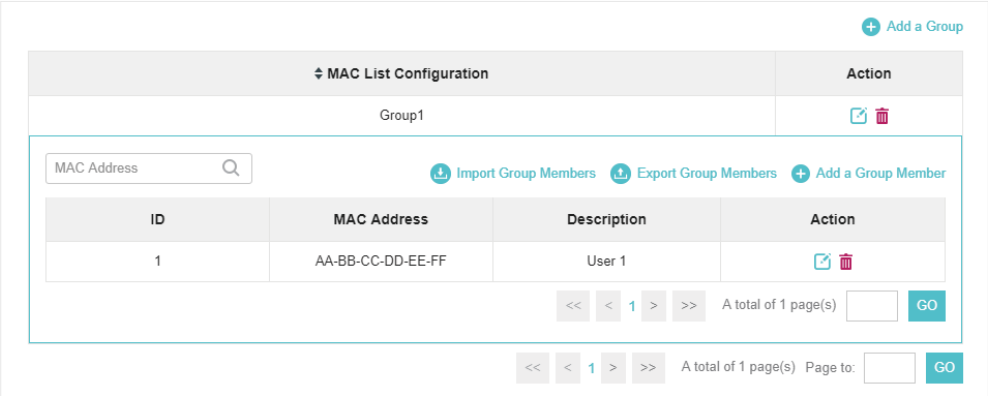


2) Click **Apply** and the group will be successfully added as shown below.



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

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

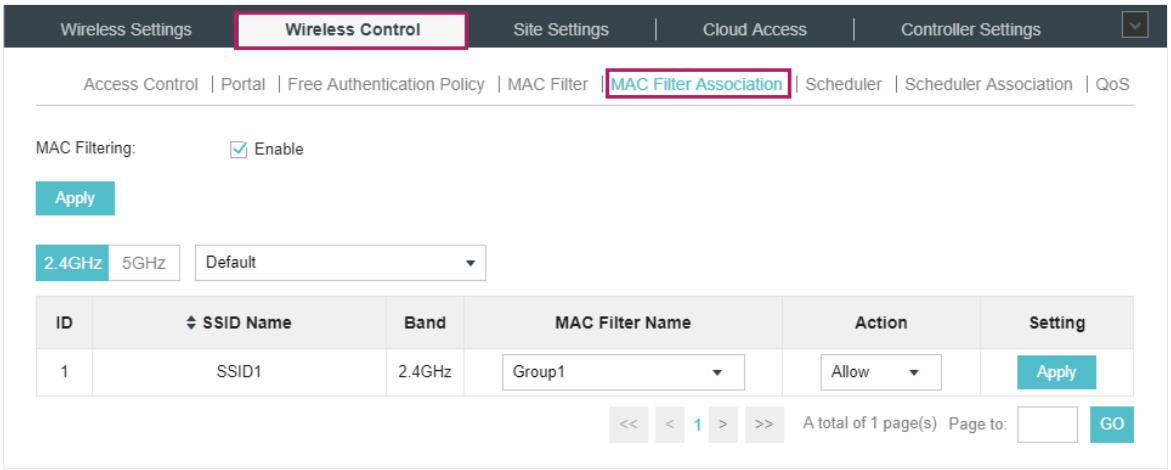


2. You can add more groups or members according to your need.

Note:

You can click Import Group Members to export the group members to a excel file and save the file on your PC. If needed, you can also click Export Group Members to import the group members to the Omada Controller.

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



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

2) Select a band frequency (2.4GHz or 5GHz) and a WLAN group.

3) In the MAC Filter Name column of the specified SSID, select a MAC Filter group in the drop-down list. Then select **Allow/Deny** in the Action column to allow/deny the clients in the MAC Filter group to access the network.

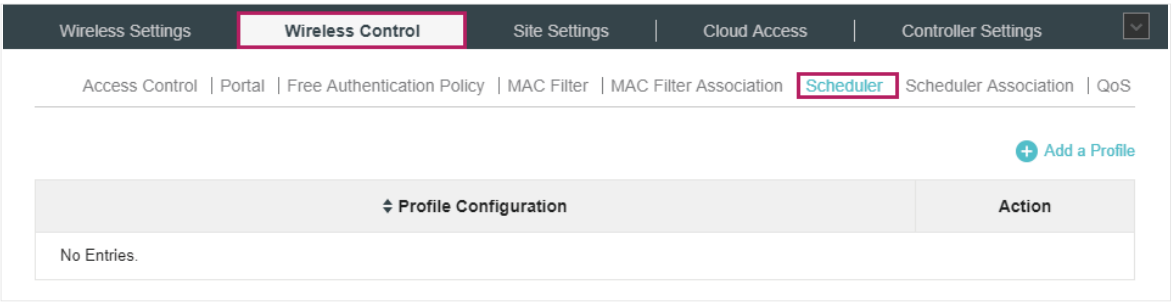
4) Click **Apply** in the Setting column.

6 Scheduler

With the Scheduler, the EAPs or its' wireless network can automatically turn on or off at the time you set. For example, you can use this feature to schedule the radio to operate only during the office working time in order to achieve security goals and reduce power consumption. You can also use the Scheduler to make clients can only access the wireless network during the time period you set in the day.

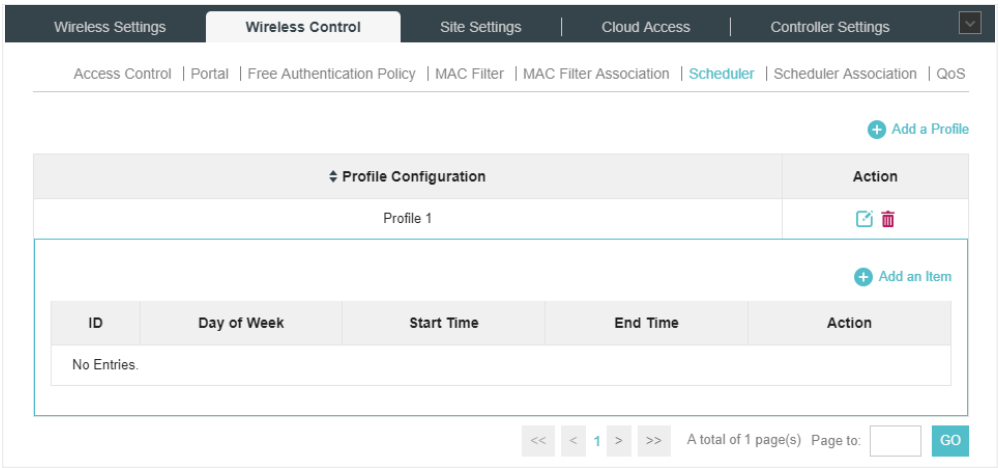
Follow the steps below to configure Scheduler.

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

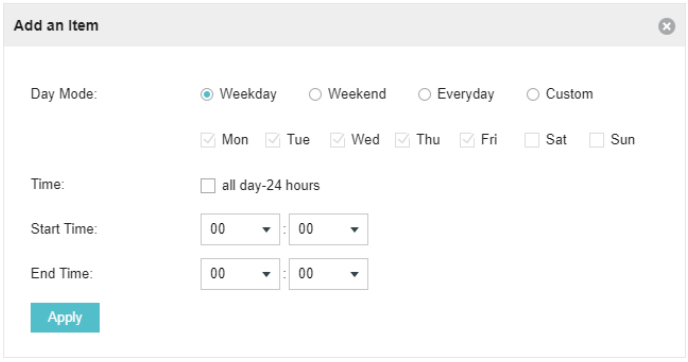


1) Click Add a Profile and specify a name for the profile.

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

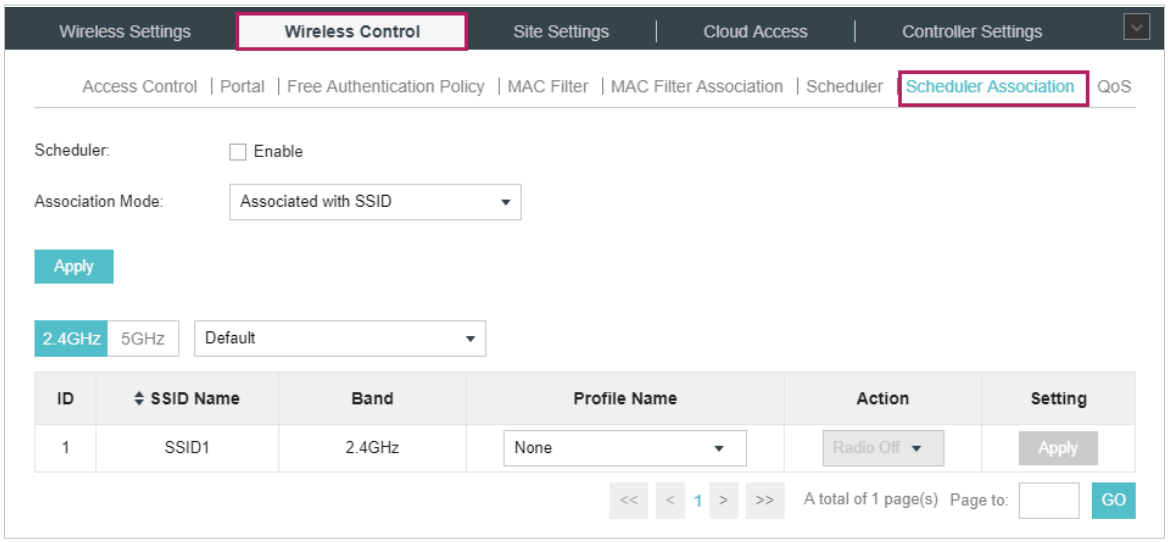


3) Click Add an Item and configure the parameters to specify a period of time.



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

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



1) Check the box to enable Scheduler function.

2) Select **Associated with SSID** (the profile will be applied to the specific SSID on all the EAPs) or **Associated with AP** (the profile will be applied to all SSIDs on the specific EAP). Then click **Apply**.

3) Select a band frequency (2.GHz or 5GHz) and a WLAN group.

4) In the Profile Name column of the specified SSID or AP, select a profile you added before in the drop-down list. Select **Radio Off/Radio On** to turn off or on the wireless network during the time interval set for the profile.

5) Click **Apply** in the Setting column.

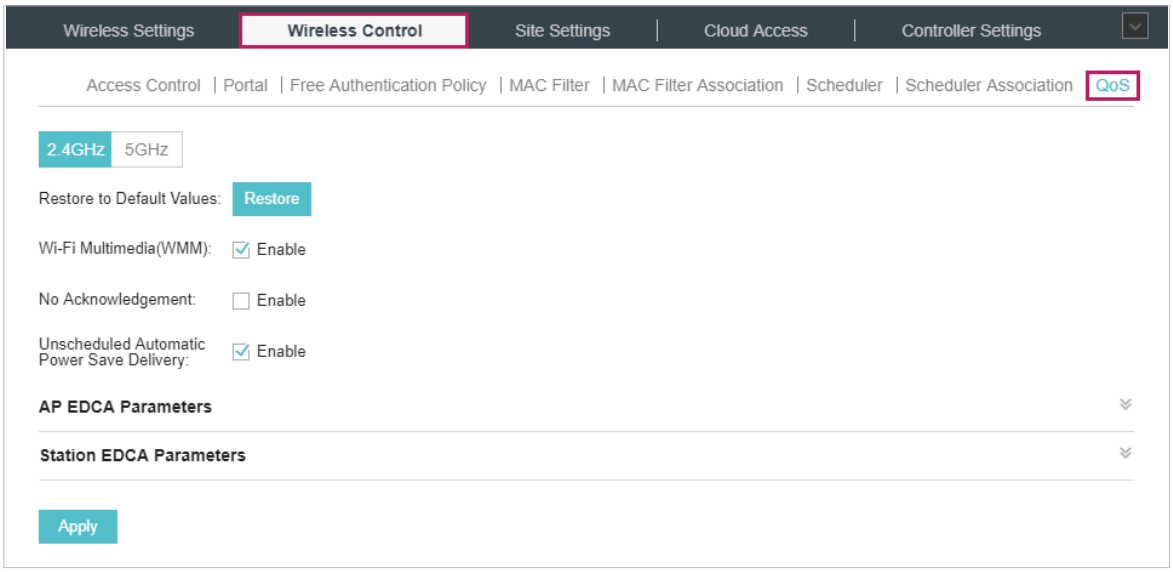
7 QoS

The Omada Controller software allows you to configure the quality of service (QoS) on the EAP for optimal throughput and performance when handling differentiated wireless traffic, such as Voice-over-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the EAP, you should set parameters on the transmission queues for different types of wireless traffic and specify minimum and maximum wait times (through contention windows) for transmission. In normal use, we recommend that you keep the default values for the EAPs and station EDCA (Enhanced Distributed Channel Access).

Follow the steps below to configure QoS.

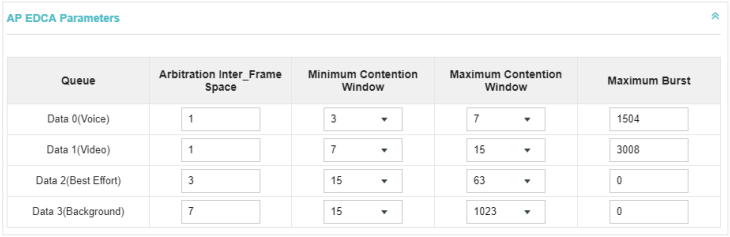
1. Go to **Wireless Control > QoS**.



2. Enable or disable the following features.

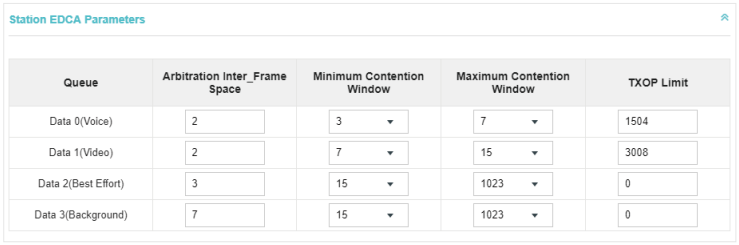
Wi-Fi Multimedia (WMM)	By default enabled. With WMM enabled, the EAPs have the QoS function to guarantee the high priority of the transmission of audio and video packets. If 802.11n only mode is selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz), the WMM should be enabled. If WMM is disabled, the 802.11n only mode cannot be selected in 2.4GHz (or 802.11n only, 802.11ac only, or 802.11 n/ac mixed mode in 5GHz).
No Acknowledgment	By default disabled. You can enable this function to specify that the EAPs should not acknowledge frames with QoS No Ack. Enabling No Acknowledgment can bring more efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
Unscheduled Automatic Power Save Delivery	By default enabled. As a power management method, it can greatly improve the energy-saving capacity of clients.

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



Queue	**Queue** displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters. **Data 0 (Voice)**—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. **Data 1 (Video)**—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. **Data 2 (Best Effort)**—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. **Data 3 (Background)**—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
Arbitration Inter-Frame Space	A wait time for data frames. The wait time is measured in slots. Valid values for **Arbitration Inter-Frame Space** are from 0 to 15.
Minimum Contention Window	A list to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. This value can not be higher than the value for the **Maximum Contention Window**.
Maximum Contention Window	The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. This value must be higher than the value for the **Minimum Contention Window**.
Maximum Burst	**Maximum Burst** specifies the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

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

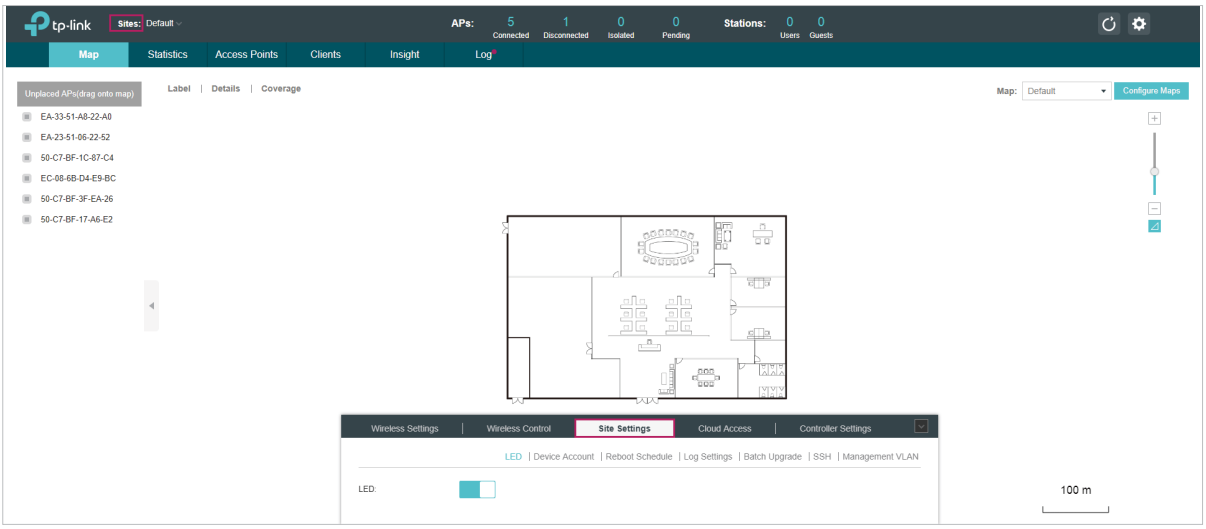


Queue	**Queue** displays the transmission queue. By default, the priority from high to low is Data 0, Data 1, Data 2, and Data 3. The priority may be changed if you reset the EDCA parameters. **Data 0 (Voice)**—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media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

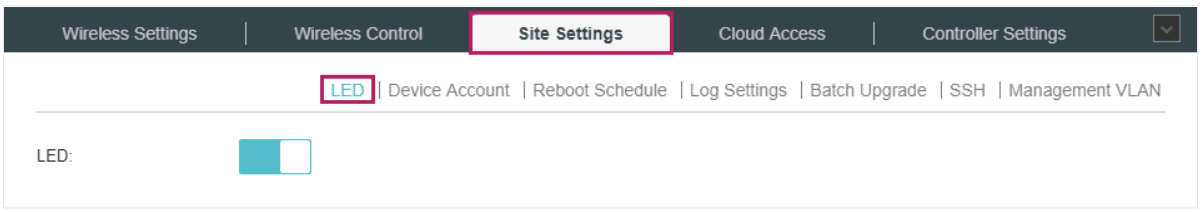
8 Site Settings

You can configure the site-specific settings on the **Site Settings** page. To switch sites, select a different site from the **Sites** drop-down menu at the top of any screen.



8.1 LED

You can change the LED light status on the EAPs on the page **Site Settings > LED**.



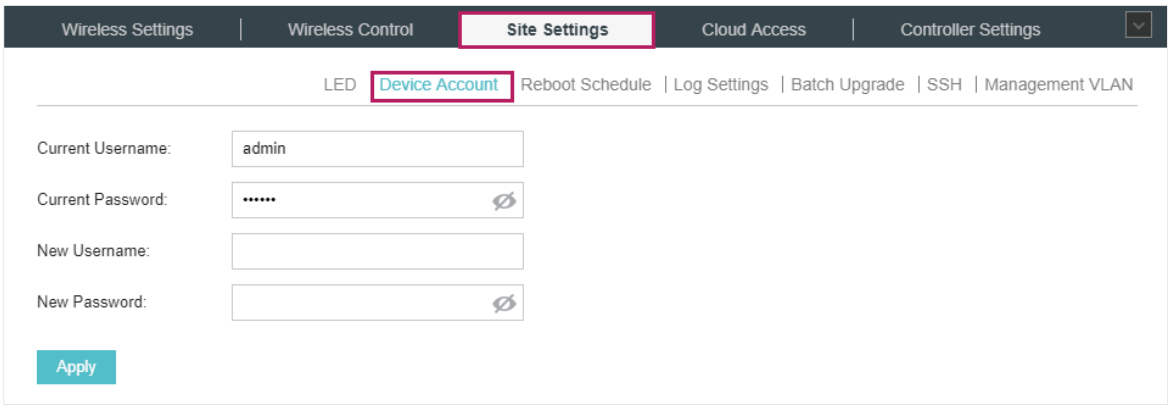
By default, the LED status is , which means that the LED lights of all the EAPs on the site are on. You can click this button to change the LED light status. The icon will be changed to , which means that all the LED lights are off.

8.2 Device Account

When the EAPs are adopted at the first time, their username and password will become the same as those of the Omada Controller which are specified at Basic Configurations. You can specify a new username and password for the adopted EAPs in batches.

Follow the steps below to change the username and password of EAPs.

1. Go to **Site Settings > Device Account.**



2. Specify a new username and password for the EAPs.

3. Click **Apply**.

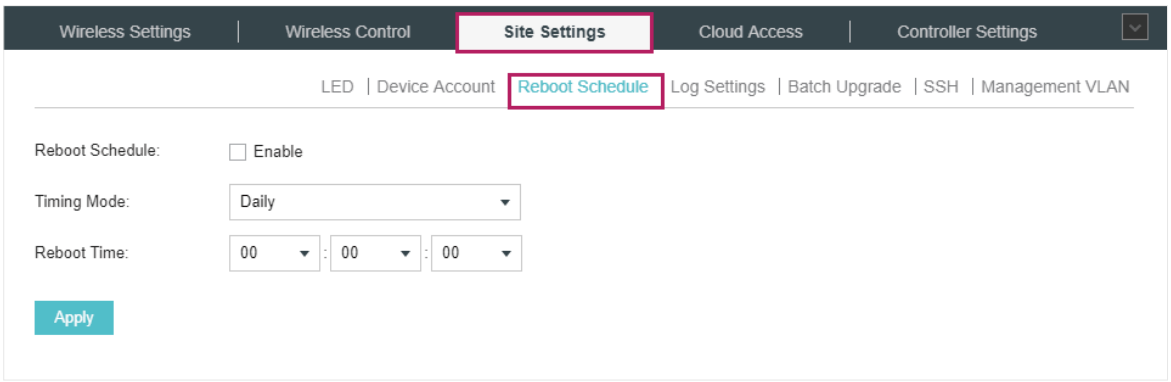
Note:

- The new account will be applied to EAPs but not the Omada Controller. To change the Omada Controller's username and password, please refer to User Account.
- Device account can be only viewed and changed when you log in to the controller as the administrator. While the operator and observer accounts do not have the permission.

8.3 Reboot Schedule

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

1. Go to **Site Settings > Reboot Schedule.**



2. Check the box to enable the function.

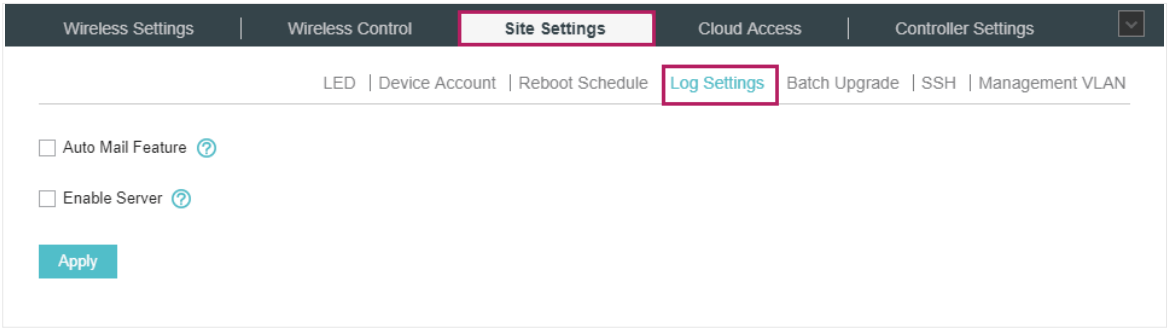
3. Choose **Daily**, **Weekly** or **Monthly** in the **Timing Mode** drop-down list and set a specific time to reboot the EAPs.

4. Click **Apply**.

8.4 Log Settings

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

1. Go to **Site Settings > Log Setting.**



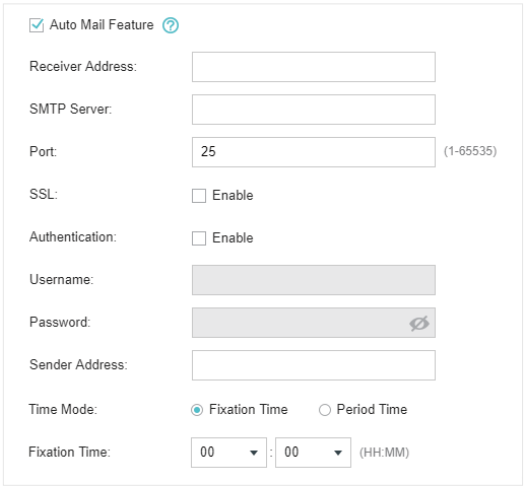
2. Check the box to choose the ways to receive system logs and click **Apply**. Two ways are available: **Auto Mail Feature** and **Server**. You can choose more than one way.

Note:

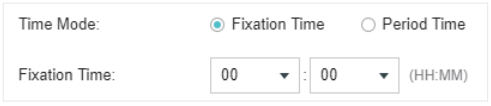
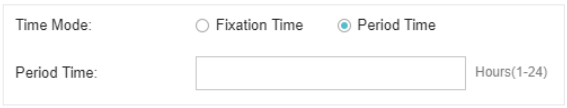
The logs and alerts of the controller with version 3.0.5 or below will be discarded after the controller is upgraded to version 3.1.4 or above.

Auto Mail Feature

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



Receiver Address	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address or domain name of the SMTP server.
Port	The SMTP server uses port 25 as default. If SSL is enabled, the port number will automatically change to 465.
SSL	You can check the box to enable SSL (Security Socket Layer) to enhance secure communications over the internet.

Authentication	You can check the box to enable mail server authentication. Enter the sender's mail account name and password.
Username	Enter the sender's mail account name.
Password	Enter the sender's mail password.
Sender Address	Enter the sender's E-mail address.
Time Mode	Select Time Mode. System logs can be sent at specific time or time interval.
Fixation Time	If you select Fixation Time, specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday. 
Period Time	If you select Period Time, specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours. 

Server

If Server is enabled, system logs will be sent to a server. Check the box to enable the feature and configure the parameters.

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.

8.5 Batch Upgrade

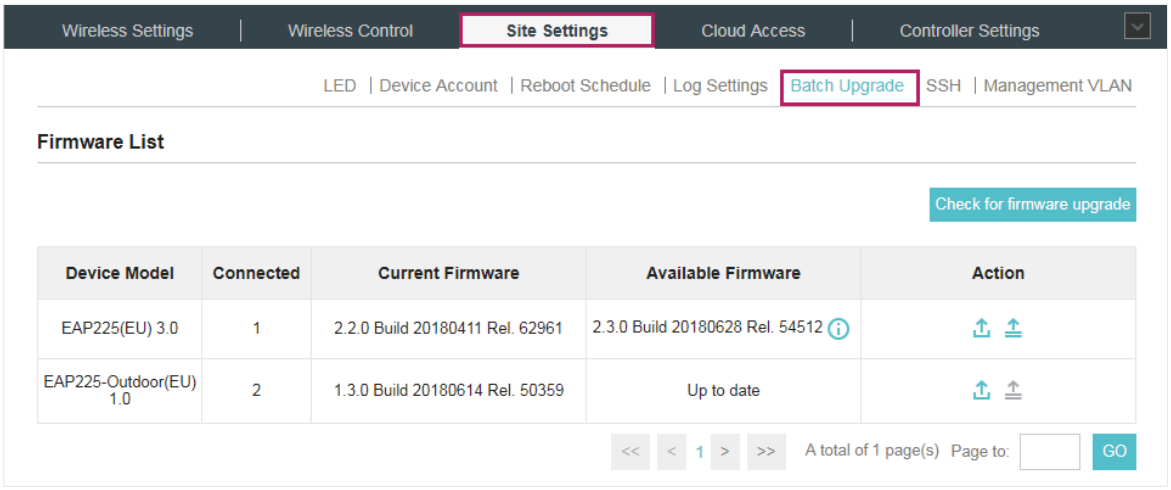
You can upgrade your EAPs of the same model in batches using Batch Upgrade. Two options are available for upgrading: upgrade online and upgrade manually.

Upgrade Online

With Cloud Access enabled, the latest firmware for the EAPs can be detected by the controller automatically. And you can upgrade the EAPs online. Thus you need not to save the firmware files locally in advance.

Follow the steps below to upgrade the EAPs online according to their model.

1. Go to **Cloud Access**. Click the button to enable Cloud Access and log in and bind with your TP-Link ID. For more details about Cloud Access, please refer to Omada Cloud Service.
2. Go to **Site Settings > Batch Upgrade**. The device model, amount, current firmware and available firmware will appear on the **Firmware list**.



3. Click in the **Action** column to upgrade the device.

After upgrading, the device will reboot automatically.

Note:

- You can click Check for firmware upgrade to check if the latest firmware is available.
- You can click in the **Available Firmware** column to view the release note of the firmware, which can help you know the new features or improvements of this firmware.

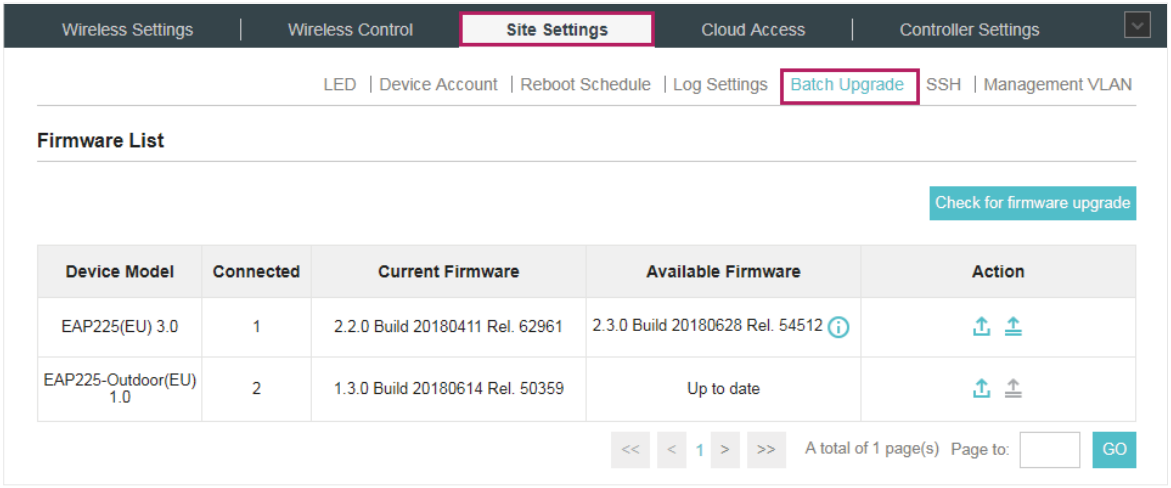
Upgrade Manually

The latest firmware files can be downloaded in the download center of TP-Link Website. Then you can upgrade the EAPs manually.

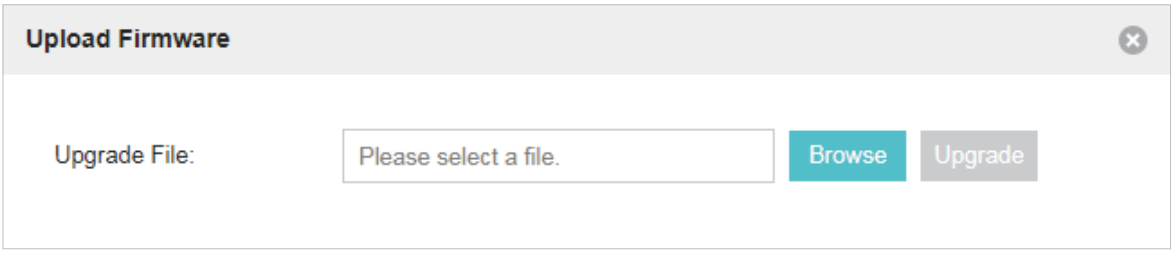
Follow the steps below to upgrade the EAPs manually according to their model.

1. Visit TP-Link Download Center to download the latest firmware file of the corresponding model.

2. Go to **Site Settings > Batch Upgrade**.



3. Click in the **Action** column to upgrade the device.



4. Click **Browse** to locate and choose the proper firmware file for the model.

5. Click **Upgrade** to upgrade the device.

After upgrading, the device will reboot automatically.

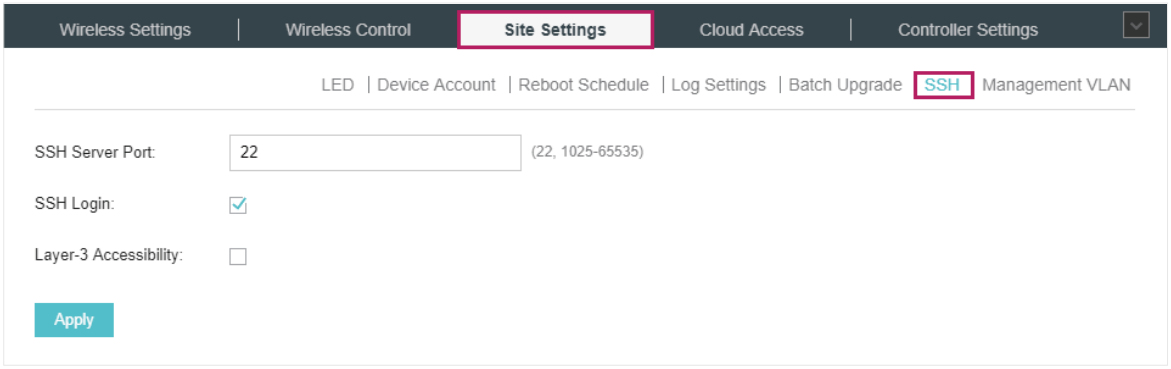
Note:

- The EAP cannot be upgraded manually when you access the controller via Omada Cloud.
- To avoid damage, please do not turn off the device while upgrading.

8.6 SSH

SSH is a protocol working in application layer and transport layer. It can provide a secure, remote connection to a device. After enabling SSH Login here, you can log in to the EAPs via SSH.

1. Go to **Site Setting > SSH**. Enter the port number of the SSH server.



2. Check the box to enable **SSH Login**. If you want to log in to the EAP from a different subnet via SSH, enable **Layer-3 Accessibility**.

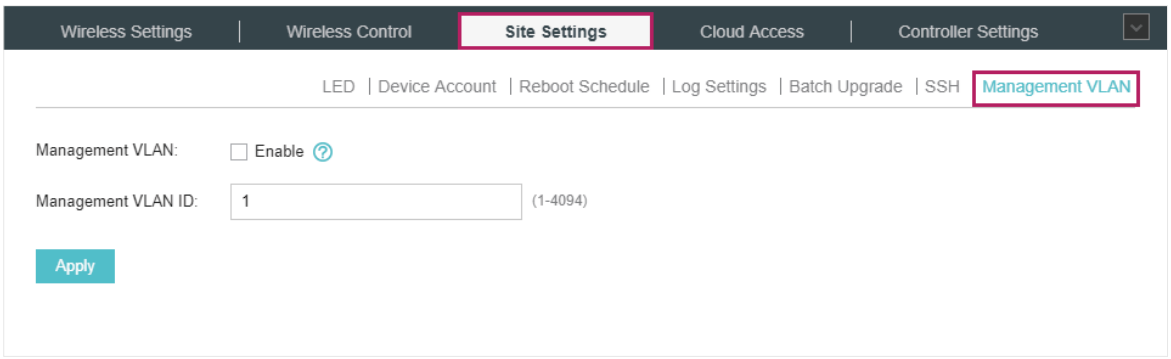
3. Click **Apply**.

8.7 Management VLAN

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

Follow the steps below to configure Management VLAN.

1. Go to **Site Setting > Management VLAN**. Check the box to enable Management VLAN.



2. Specify the Management VLAN ID. The default VLAN ID is 1.

3. Click **Apply**.