Configure WLAN for EAP via Omada Controller

CONTENTS

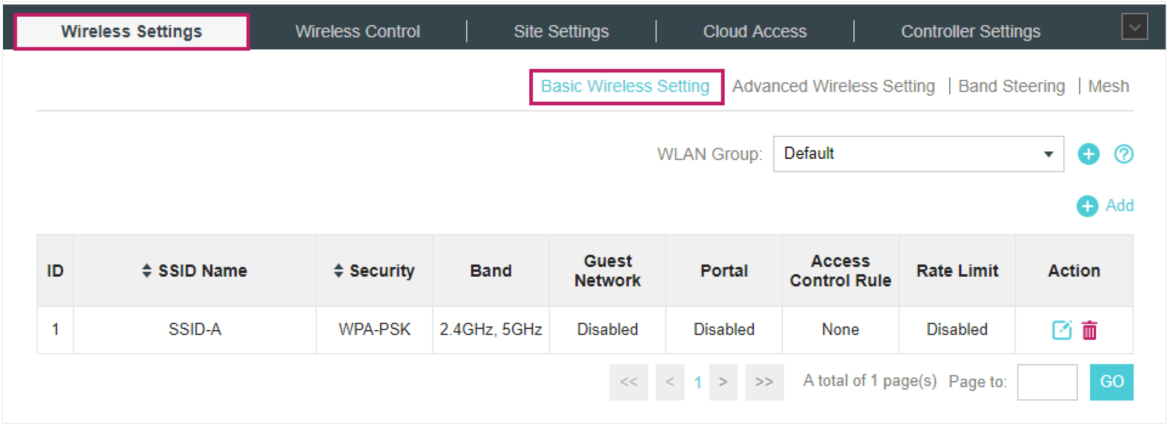
1 Overview

In addition to the wireless network you created in Quick Start, you can add more wireless networks by configuring the basic and advanced wireless parameters. Also, you can improve the network quality by configuring Band Steering and expand your wireless network by configuring Mesh on other EAPs.

2 Configure Basic Wireless Parameters

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

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



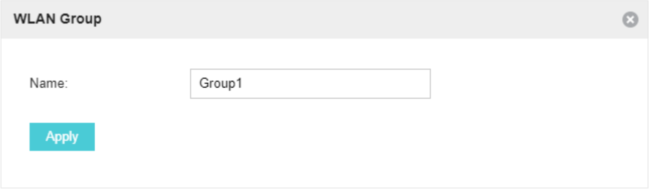
WLAN Group: Default

ID	SSID Name	Security	Band	Guest Network	Portal	Access Control Rule	Rate Limit	Action
1	SSID-A	WPA-PSK	2.4GHz, 5GHz	Disabled	Disabled	None	Disabled	

A total of 1 page(s) Page to:

2. Click ⊕ at the right of WLAN Group: Default ▾ 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.

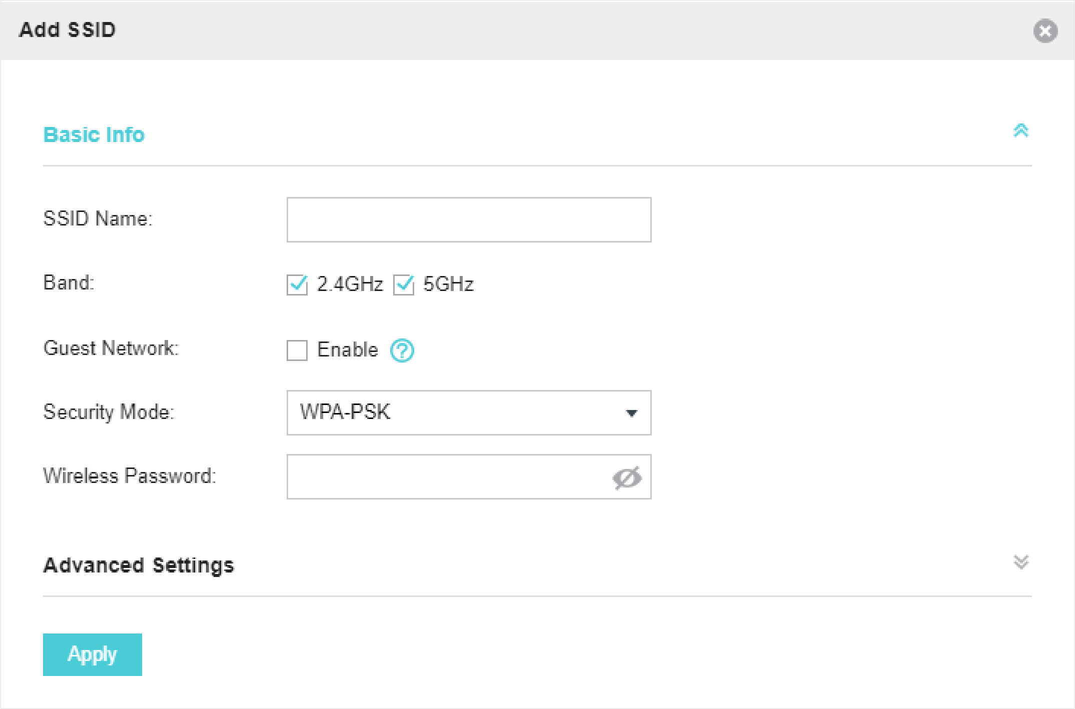
3. Specify a name for the group and click **Apply**.



Name: Group1

4. Select the WLAN group WLAN Group: Default ▾ and click ⊕ Add to add an SSID to the specific WLAN group.

5. Configure the parameters in the following window.



Add SSID

Basic Info

SSID Name:

Band: ☑ 2.4GHz ☑ 5GHz

Guest Network: □ Enable

Security Mode: WPA-PSK

Wireless Password:

Advanced Settings

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.

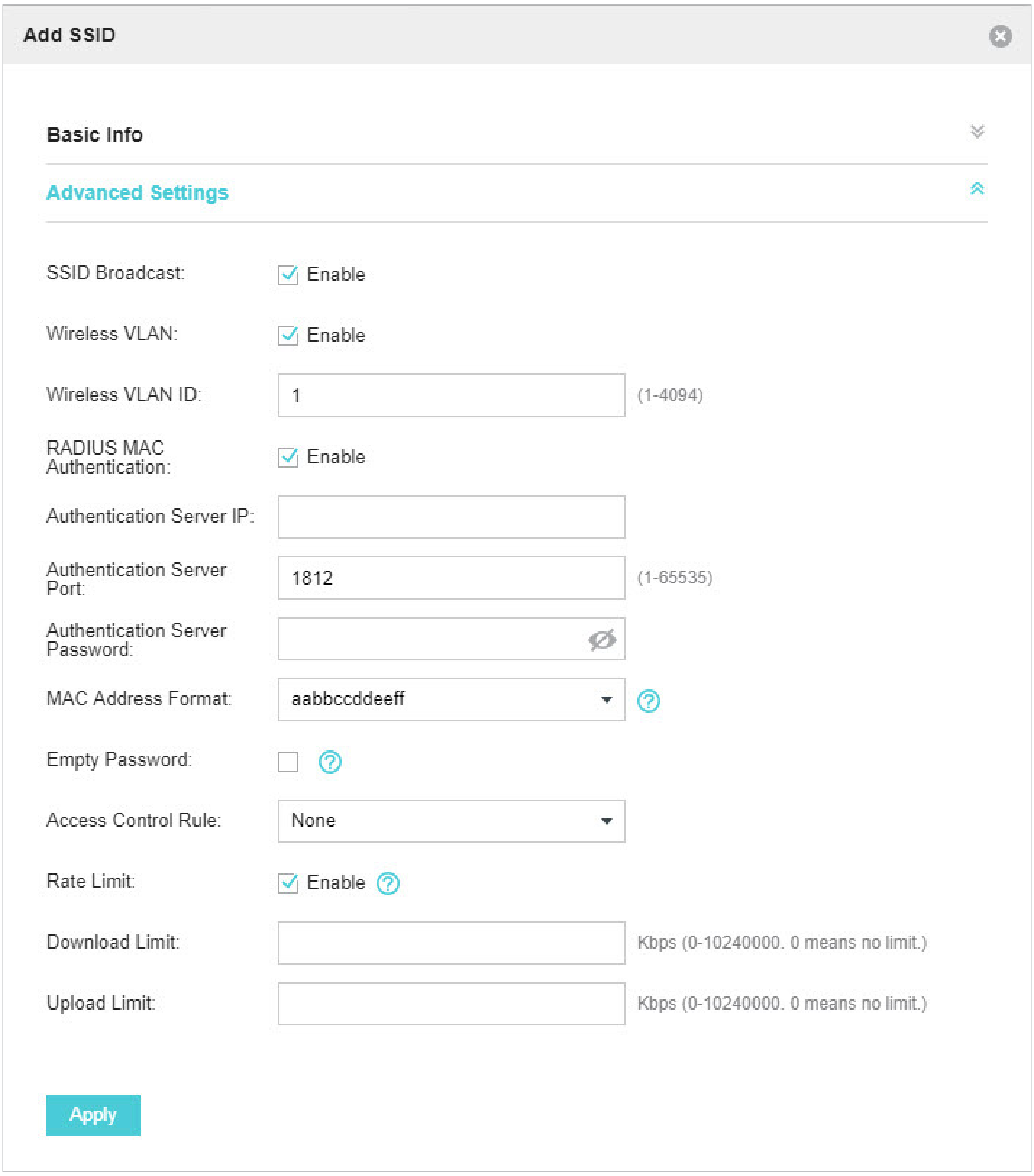
Note:

- 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.



Add SSID

Basic Info

Advanced Settings

SSID Broadcast: ☑ Enable

Wireless VLAN: ☑ Enable

Wireless VLAN ID: 1 (1-4094)

RADIUS MAC Authentication: ☑ Enable

Authentication Server IP:

Authentication Server Port: 1812 (1-65535)

Authentication Server Password:

MAC Address Format: aabbccddeeff

Empty Password: □

Access Control Rule: None

Rate Limit: ☑ Enable

Download Limit: Kbps (0-10240000. 0 means no limit.)

Upload Limit: Kbps (0-10240000. 0 means no limit.)

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.

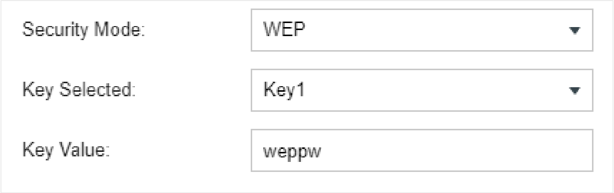
Wireless VLAN	With this option enabled, the EAP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot 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.



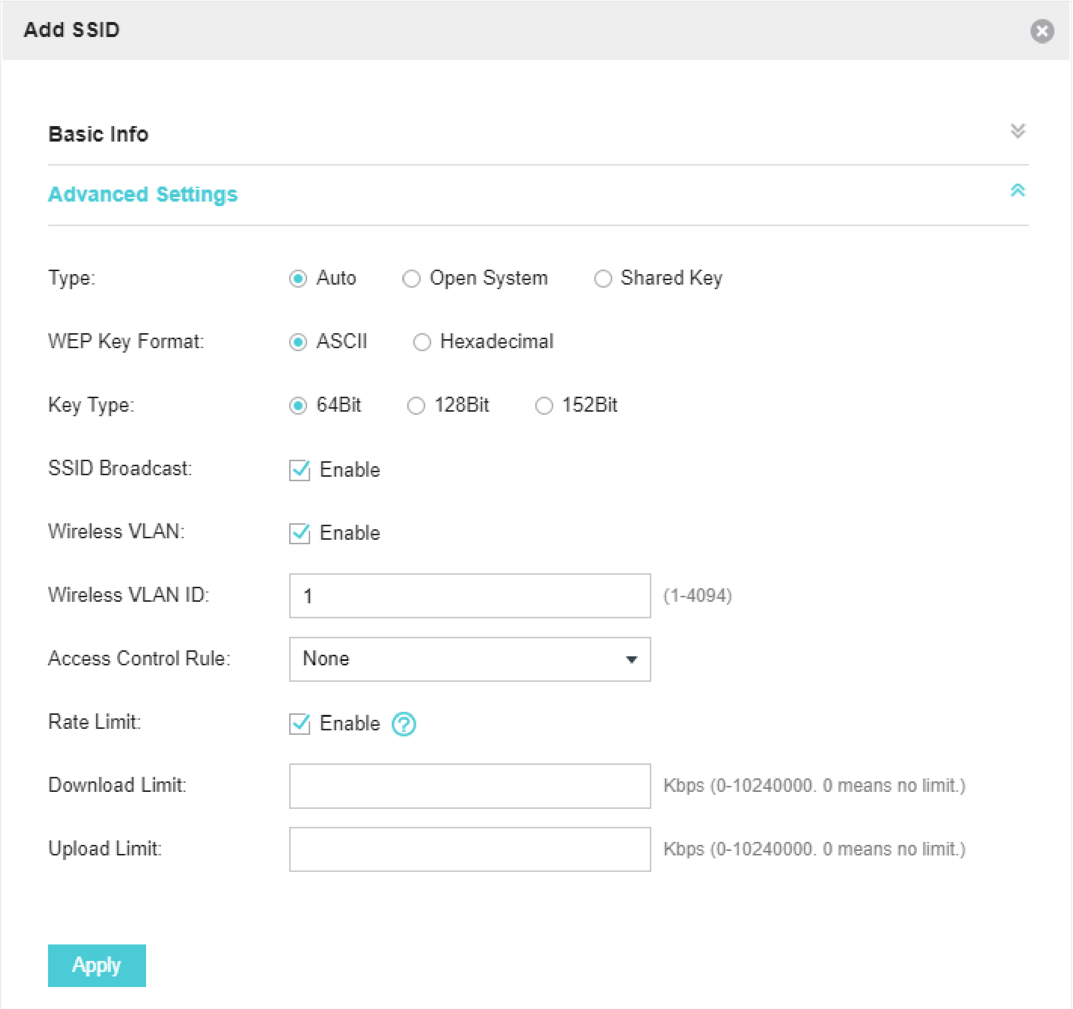
Security Mode: WEP

Key Selected: Key1

Key Value: weppw

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: ● Auto ○ Open System ○ Shared Key

WEP Key Format: ● ASCII ○ Hexadecimal

Key Type: ● 64Bit ○ 128Bit ○ 152Bit

SSID Broadcast: ☑ Enable

Wireless VLAN: ☑ Enable

Wireless VLAN ID: 1 (1-4094)

Access Control Rule: None

Rate Limit: ☑ Enable

Download Limit: Kbps (0-10240000. 0 means no limit.)

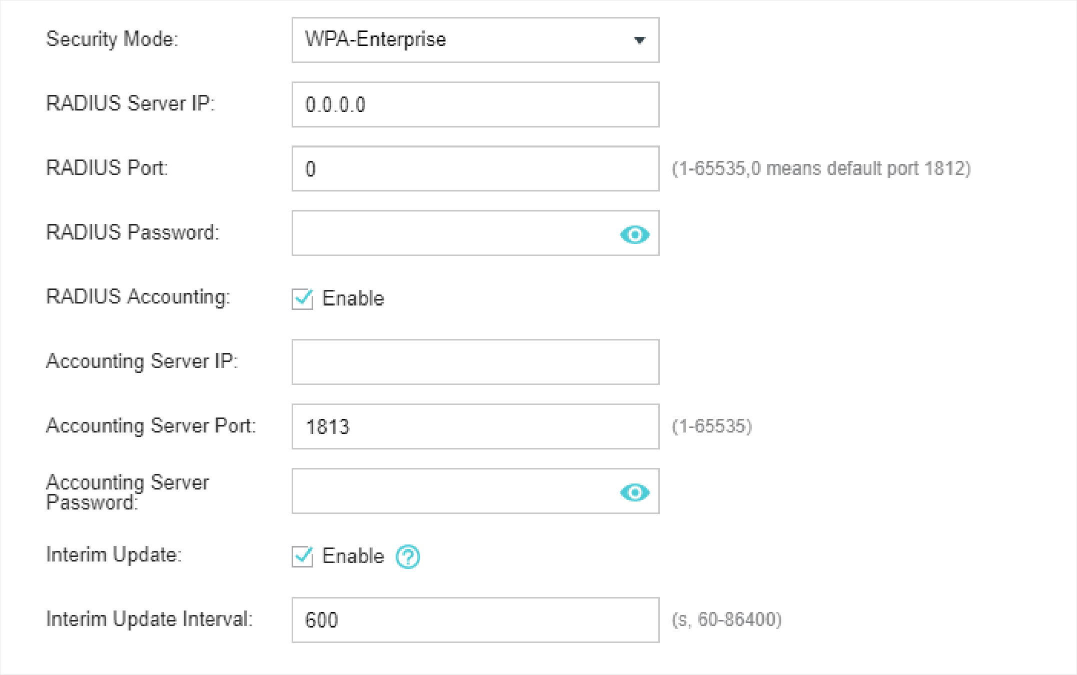
Upload Limit: Kbps (0-10240000. 0 means no limit.)

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

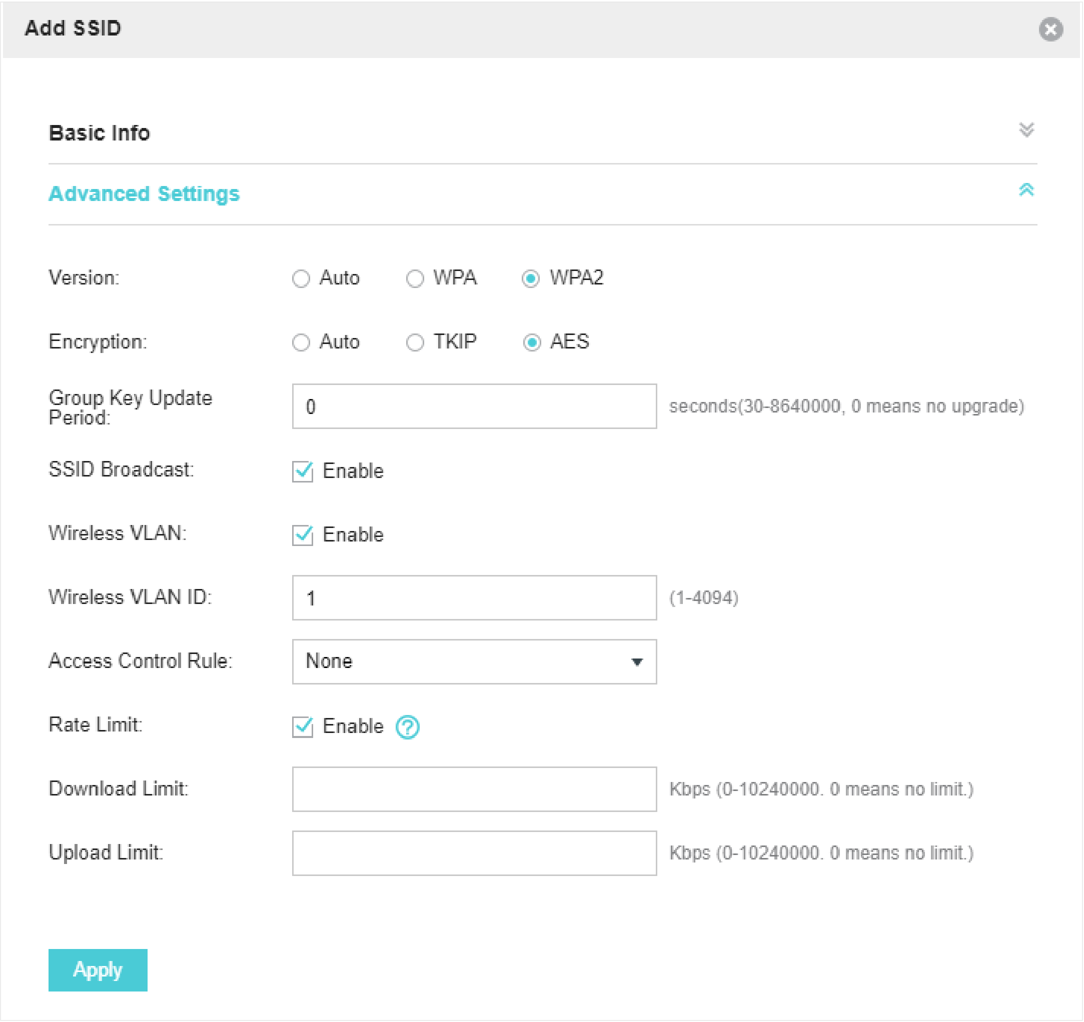
The WPA-Enterprise mode requires a RADIUS server to authenticate clients. Since the WPA-Enterprise can generate different passwords for different clients, it is much safer than WPA-PSK. However, it costs much more to maintain and is usually used by enterprise.



Security Mode:	WPA-Enterprise	
RADIUS Server IP:	0.0.0.0	
RADIUS Port:	0	(1-65535,0 means default port 1812)
RADIUS Password:		
RADIUS Accounting:	☑ Enable	
Accounting Server IP:		
Accounting Server Port:	1813	(1-65535)
Accounting Server Password:		
Interim Update:	☑ Enable	
Interim Update Interval:	600	(s, 60-86400)

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: ○ Auto ○ WPA ● WPA2

Encryption: ○ Auto ○ TKIP ● AES

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

SSID Broadcast: ☑ Enable

Wireless VLAN: ☑ Enable

Wireless VLAN ID: 1 (1-4094)

Access Control Rule: None

Rate Limit: ☑ Enable

Download Limit: Kbps (0-10240000. 0 means no limit.)

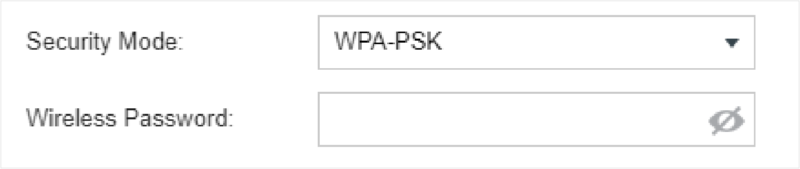
Upload Limit: Kbps (0-10240000. 0 means no limit.)

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.

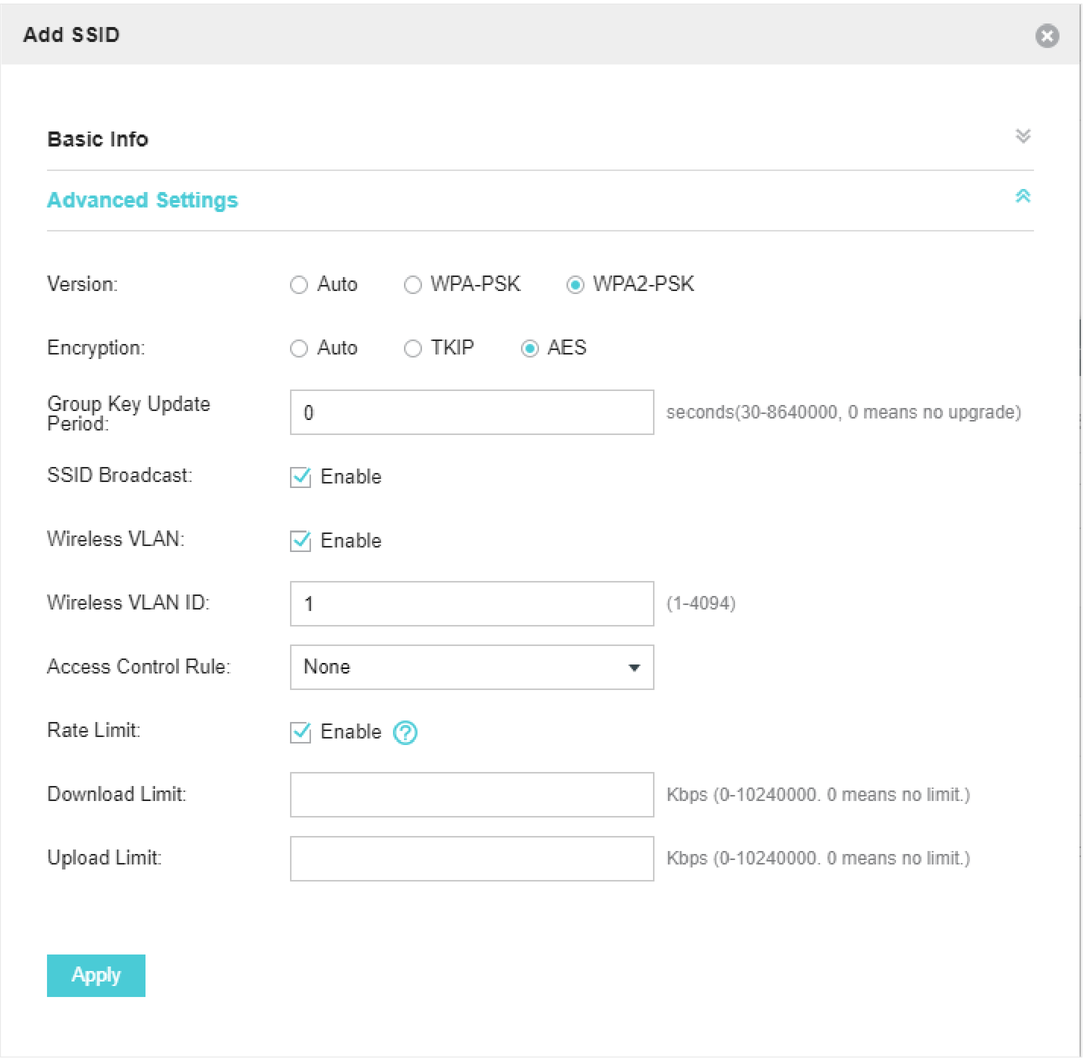


Security Mode: WPA-PSK

Wireless Password:

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.



Add SSID

Basic Info

Advanced Settings

Version: ○ Auto ○ WPA-PSK ● WPA2-PSK

Encryption: ○ Auto ○ TKIP ● AES

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

SSID Broadcast: ☑ Enable

Wireless VLAN: ☑ Enable

Wireless VLAN ID: 1 (1-4094)

Access Control Rule: None

Rate Limit: ☑ Enable

Download Limit: Kbps (0-10240000. 0 means no limit.)

Upload Limit: Kbps (0-10240000. 0 means no limit.)

Apply

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.

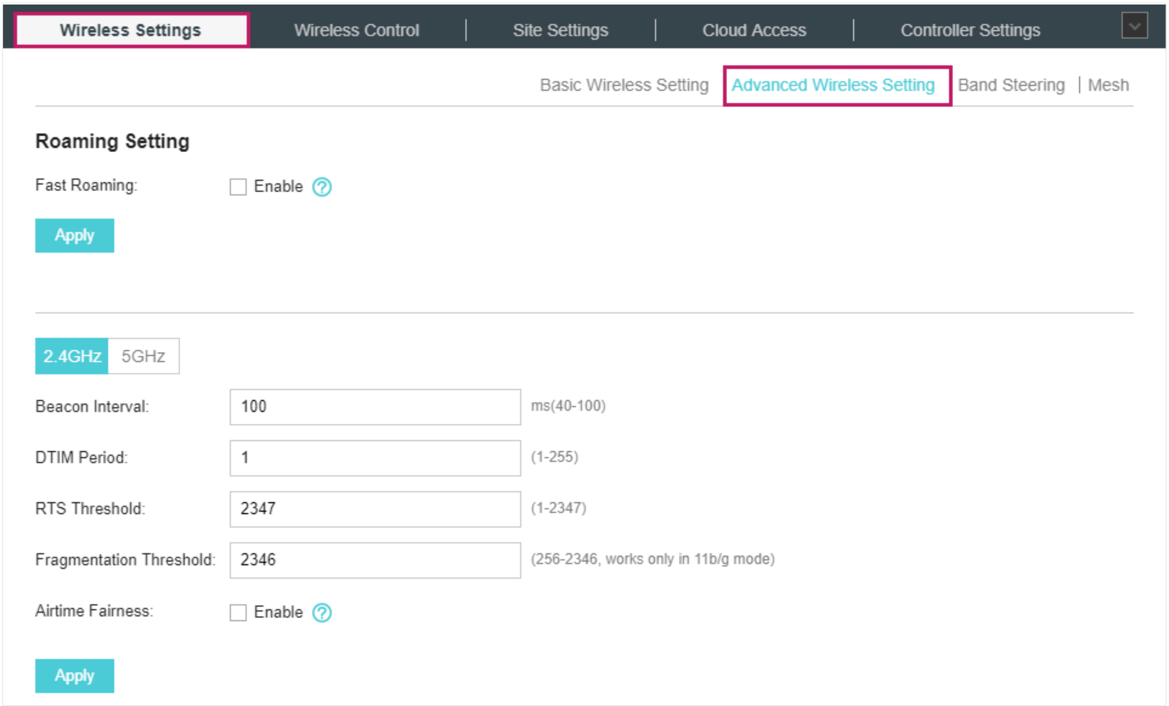
6. Click **Apply.**

3 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.**



Roaming Setting

Fast Roaming: □ Enable

Beacon Interval: 100 ms(40-100)

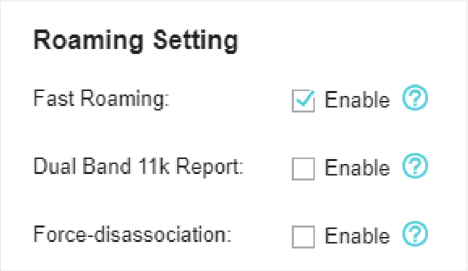
DTIM Period: 1 (1-255)

RTS Threshold: 2347 (1-2347)

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

Airtime Fairness: □ Enable

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



Roaming Setting

Fast Roaming: ☑ Enable

Dual Band 11k Report: □ Enable

Force-disassociation: □ Enable

Fast Roaming	With this option enabled, 11k/v capable clients can have improved fast roaming experience when moving among different APs.
Dual Band 11k Report	With this feature disabled, the controller provides candidate AP report that contains the APs in the same band as the clients. With this feature enabled, the controller provides candidate AP report that contains the APs in both 2.4GHz and 5GHz bands.
Force-disassociation	The controller dynamically monitors the link quality of every associated client. When the client's current link quality drops below the predefined threshold and there are some other APs with better signal, the current AP issues an 11v roaming suggestion to the client. With Force-disassociation disabled, the AP only issues a roaming suggestion, but whether to roam or not is determined by the client. With Force-disassociation enabled, the AP not only issues a roaming suggestion but also disassociates the client after a while. Thus the client is supported to re-associate to a better AP. This function is recommended when there are sticky clients that don't roam.

3. Click **Apply**.

4. Select the band frequency 2.4GHz 5GHz.

5. Configure the following parameters.

Beacon Interval	Beacons are transmitted periodically by the EAP 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.

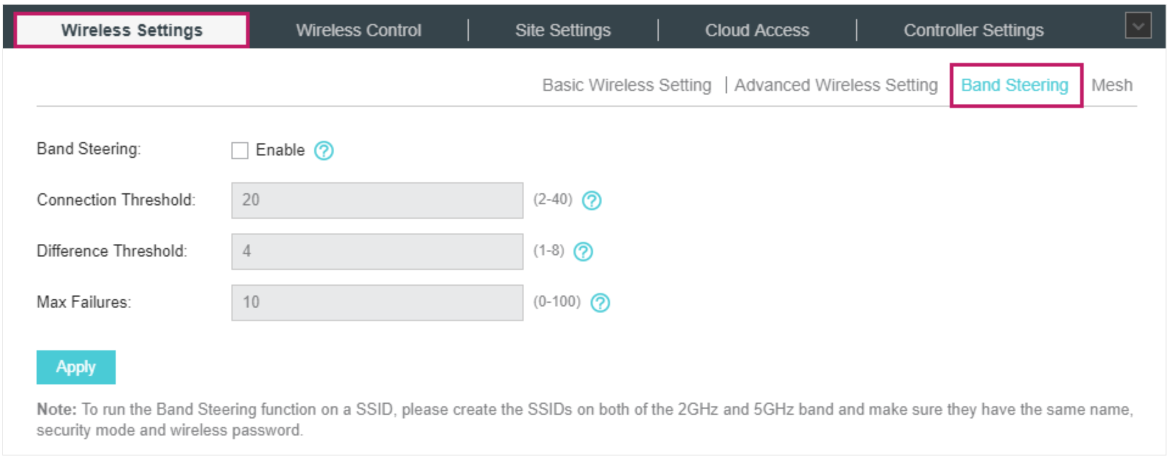
6. Click **Apply**.

4 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.**



Band Steering: □ Enable

Connection Threshold: 20 (2-40)

Difference Threshold: 4 (1-8)

Max Failures: 10 (0-100)

Note: To run the Band Steering function on a SSID, please create the SSIDs on both of the 2GHz and 5GHz band and make sure they have the same name, security mode and wireless password.

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**.

5 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.

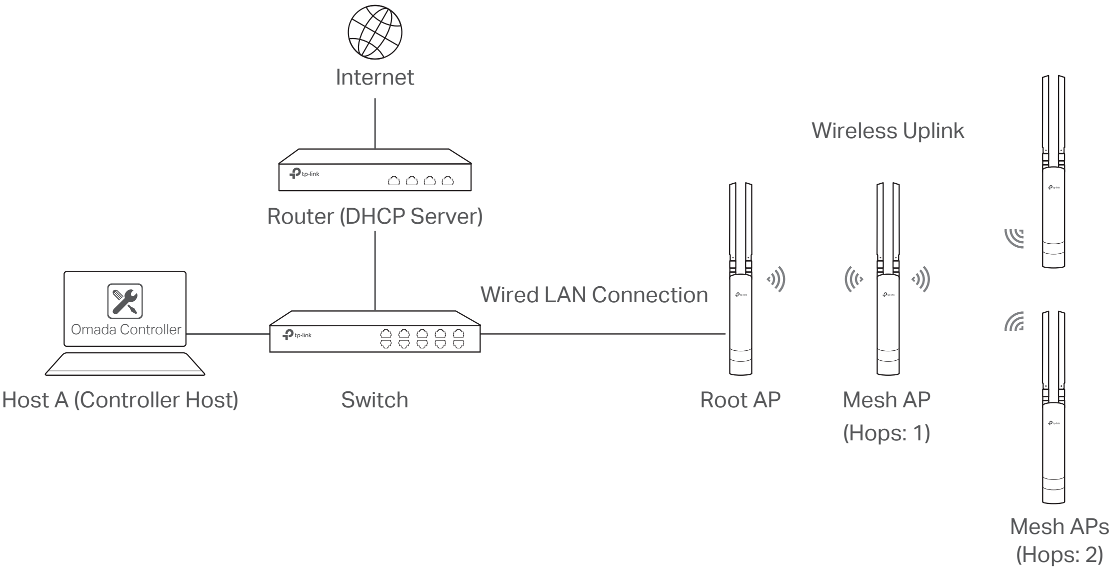
Note:

- 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.

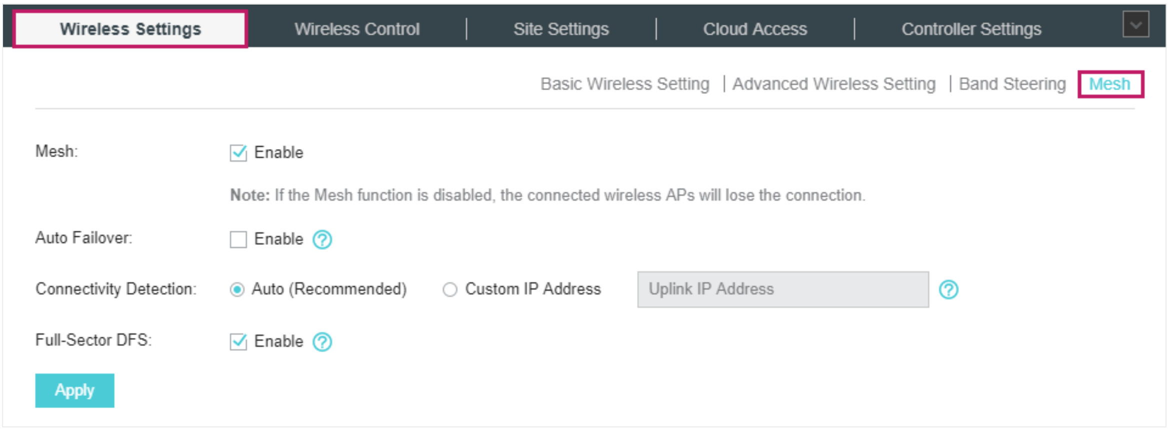


After all the EAPs are adopted, a mesh network is established. Then the EAPs connected to the network wirelessly also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

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.**



Mesh: ☑ Enable

Note: If the Mesh function is disabled, the connected wireless APs will lose the connection.

Auto Failover: □ Enable

Connectivity Detection: ● Auto (Recommended) ○ Custom IP Address Uplink IP Address

Full-Sector DFS: ☑ Enable

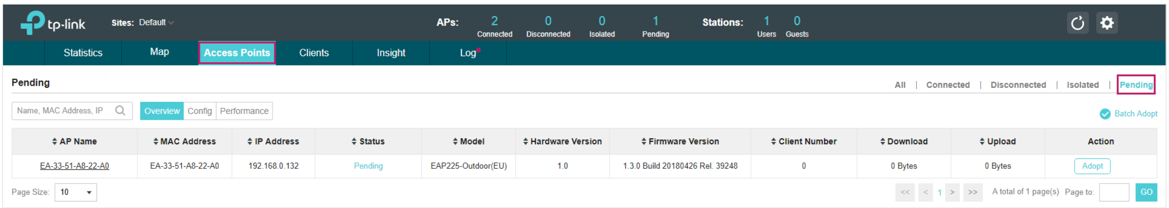
2. Check the box to enable the Mesh function.

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.

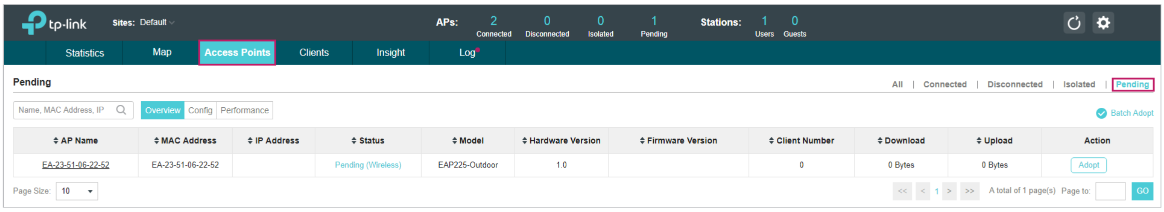


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 1 Users 0 Guests
Statistics
Map
Access Points
Clients
Insight
Log
Pending
All | Connected | Disconnected | Isolated | Pending
Name, MAC Address, IP
Overview
Config
Performance
Batch Adopt
Page Size: 10
<< < 1 > >>
A total of 1 page(s) Page to:
GO

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
EA-33-51-A8-22-A0	EA-33-51-A8-22-A0	192.168.0.132	Pending	EAP225-Outdoor(EU)	1.0	1.3.0 Build 20180426 Rel. 39248	0	0 Bytes	0 Bytes	Adopt

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.

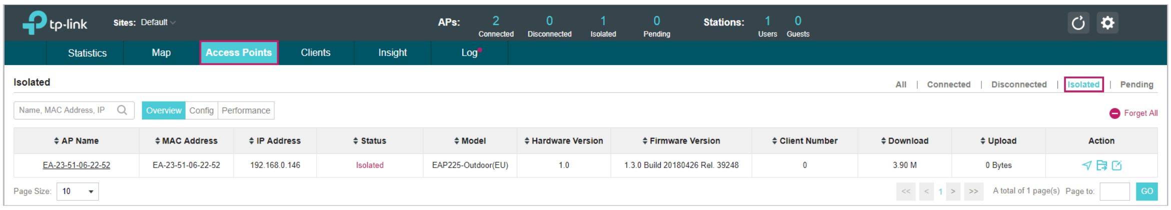


tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 0 Isolated 1 Pending
Stations: 1 Users 0 Guests
Statistics
Map
Access Points
Clients
Insight
Log
Pending
All | Connected | Disconnected | Isolated | Pending
Name, MAC Address, IP
Overview
Config
Performance
Batch Adopt
Page Size: 10
<< < 1 > >>
A total of 1 page(s) Page to:
GO

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
EA-23-51-06-22-52	EA-23-51-06-22-52		Pending (Wireless)	EAP225-Outdoor	1.0		0	0 Bytes	0 Bytes	Adopt

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.

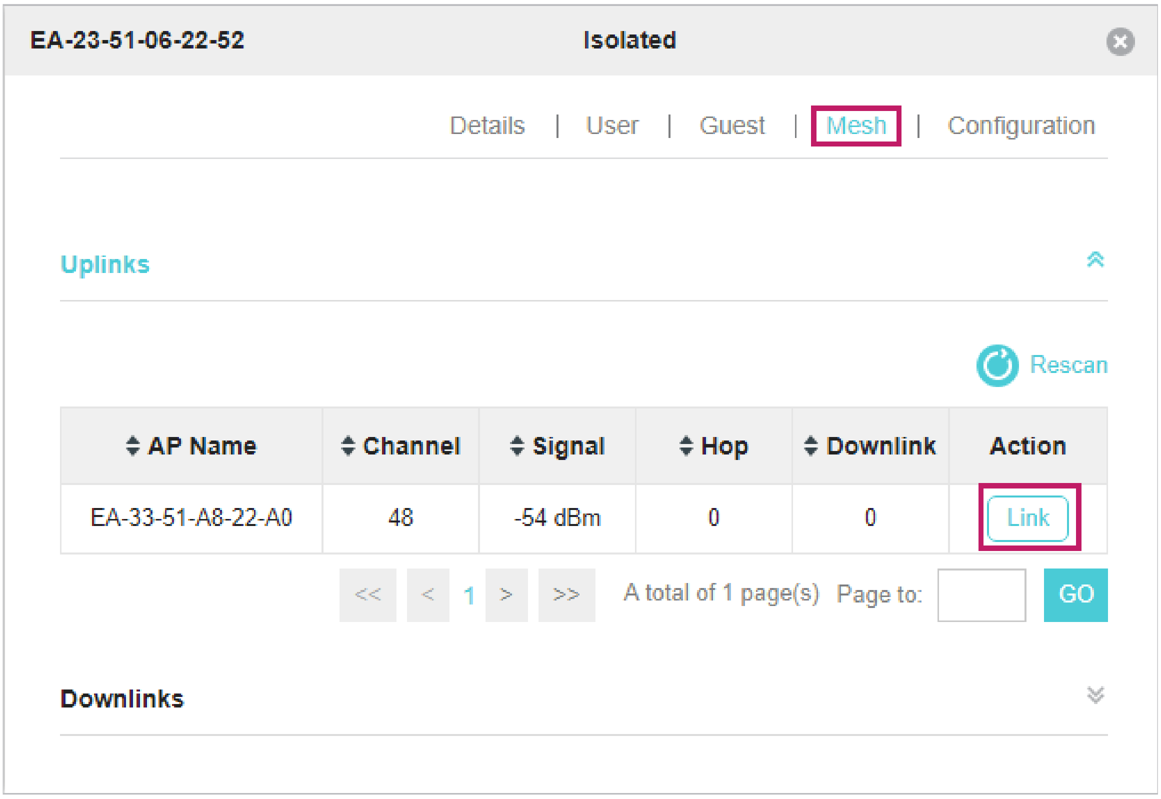
2) For the EAP that has been managed by Omada Controller before and cannot reach the gateway, it goes into Isolated status when it is discovered by controller again. Go to **Access Points > Isolated**, click ✎.



tp-link
Sites: Default
APs: 2 Connected 0 Disconnected 1 Isolated 0 Pending
Stations: 1 Users 0 Guests
Statistics
Map
Access Points
Clients
Insight
Log
Isolated
All | Connected | Disconnected | Isolated | Pending
Name, MAC Address, IP
Overview
Config
Performance
Forget All
Page Size: 10
<< < 1 > >> A total of 1 page(s) Page to: GO

AP Name	MAC Address	IP Address	Status	Model	Hardware Version	Firmware Version	Client Number	Download	Upload	Action
EA-23-51-06-22-52	EA-23-51-06-22-52	192.168.0.146	Isolated	EAP225-Outdoor(EU)	1.0	1.3.0 Build 20180426 Rel. 39248	0	3.90 M	0 Bytes	

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



EA-23-51-06-22-52
Isolated
Details | User | Guest | Mesh | Configuration
Uplinks
Rescan
<< < 1 > >> A total of 1 page(s) Page to: GO
Downlinks

AP Name	Channel	Signal	Hop	Downlink	Action
EA-33-51-A8-22-A0	48	-54 dBm	0	0	Link

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

Tips:

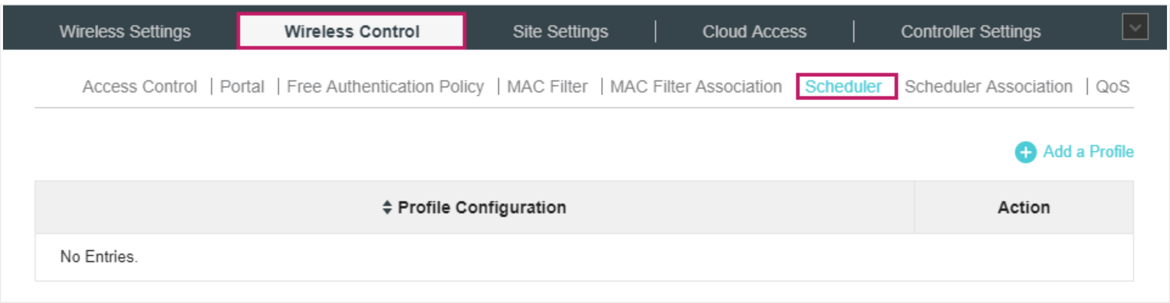
- You can manually select the uplink AP that you want to connect in the uplink EAP list. To build a mesh network with better performance, we recommend that you select the Uplink AP with the strongest signal, least hop and least Downlink AP.
- You can enable **Auto Failover** to make the controller automatically 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.

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.

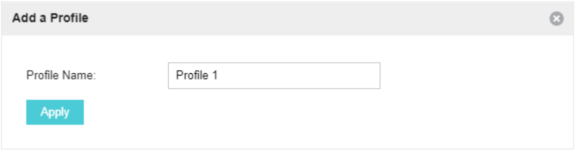
Follow the steps below to configure Scheduler.

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



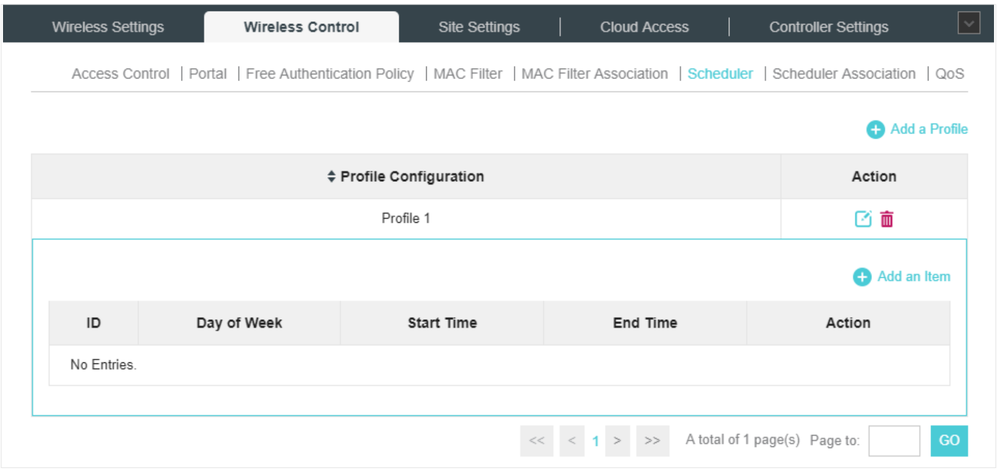
≑ Profile Configuration	Action
No Entries.	

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



Profile Name: Profile 1

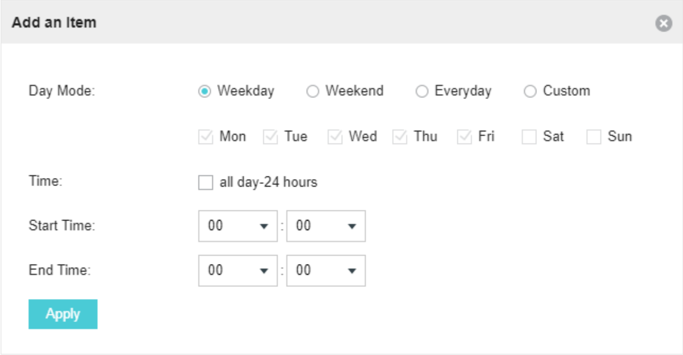
2) Click **Apply** and the profile will be added.



≑ Profile Configuration	Action
Profile 1	

ID	Day of Week	Start Time	End Time	Action
No Entries.				

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



Add an Item

Day Mode: ● Weekday ○ Weekend ○ Everyday ○ Custom

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

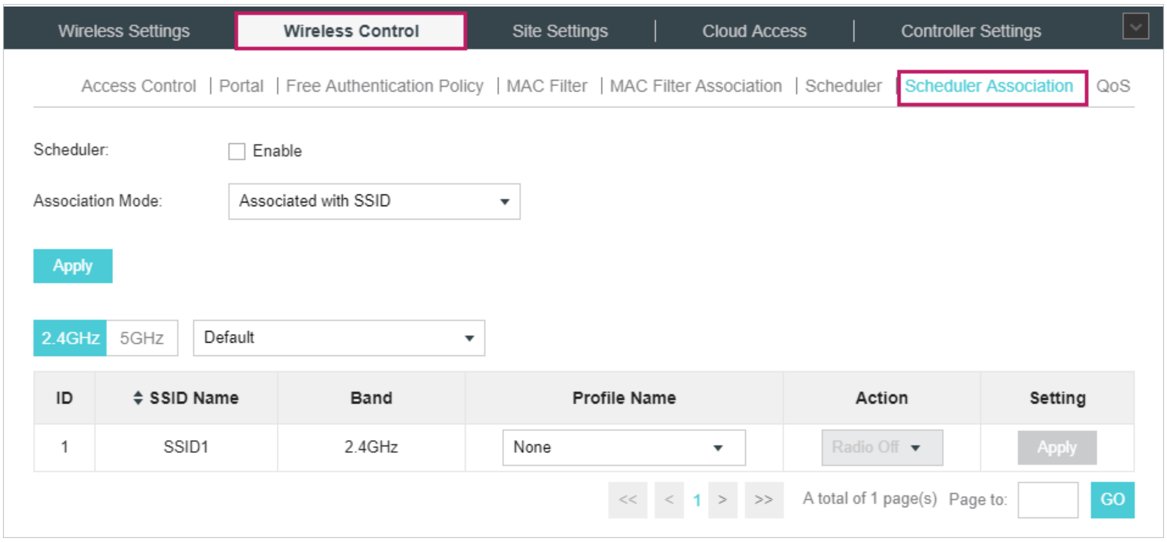
Time: □ all day-24 hours

Start Time: 00 : 00

End Time: 00 : 00

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

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



Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings
Access Control | Portal | Free Authentication Policy | MAC Filter | MAC Filter Association | Scheduler | Scheduler Association | QoS

Scheduler: □ Enable

Association Mode: Associated with SSID

Apply
2.4GHz 5GHz
Default

ID	SSID Name	Band	Profile Name	Action	Setting
1	SSID1	2.4GHz	None	Radio Off	Apply

<< < 1 > >>
A total of 1 page(s) Page to:
GO

1) Check the box to enable Scheduler function.

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

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

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

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