antaira®

making connectivity simple...

ARS/X/Y-7234 Industrial Wireless Software User's Manual

Version 1.0
(December 2018)

Trademark Information

Antaira is a registered trademark of Antaira Technologies, LLC., Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Antaira Technologies, LLC. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC. will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC Notice

This equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

CE Mark Warning

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

Industrial Wireless APs

Software User's Manual

This manual supports the following models:

- ARS-7234-AC-T
- ARX-7234-AC-PD-T
- ARY-7234-AC-PD

Please check our website (www.antaira.com) for any updated manual or contact us by e-mail (support@antaira.com).

Table of Contents

1. Access with Web Browser

1.1 Web GUI Login

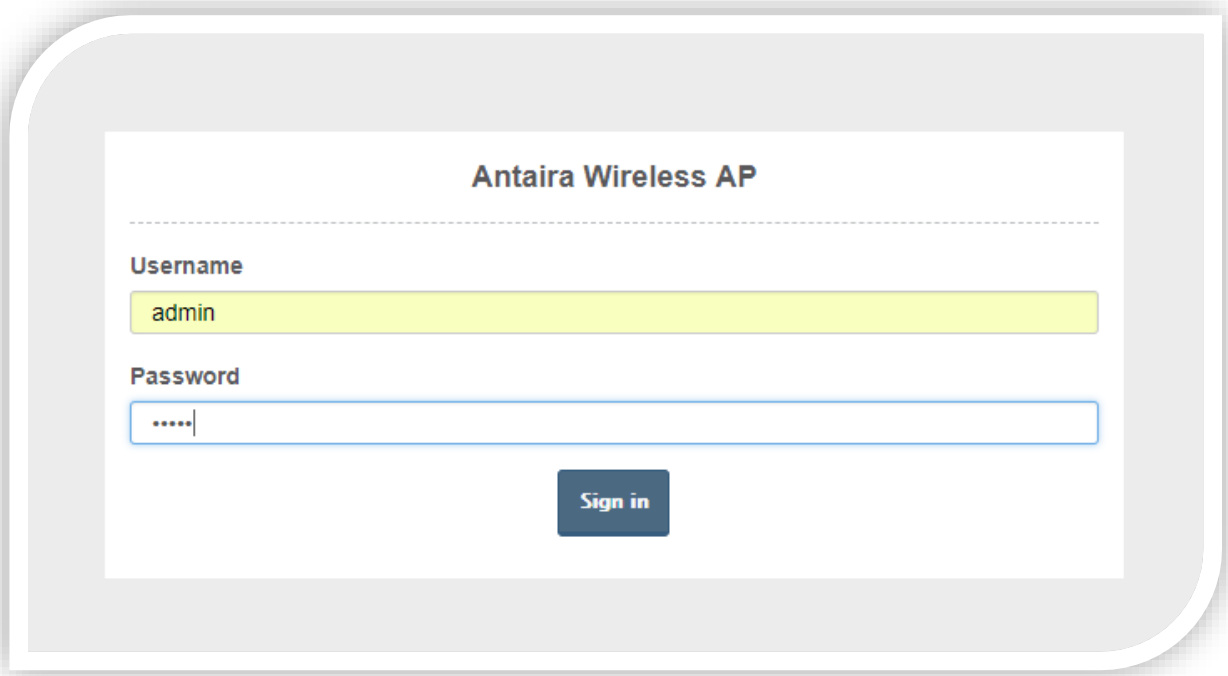
Step 1: To access the WEB GUI, open a web browser and type the following IP address: http://192.168.1.254

Step 2: The default WEB GUI Login:

Username: **admin**

Password: **admin**

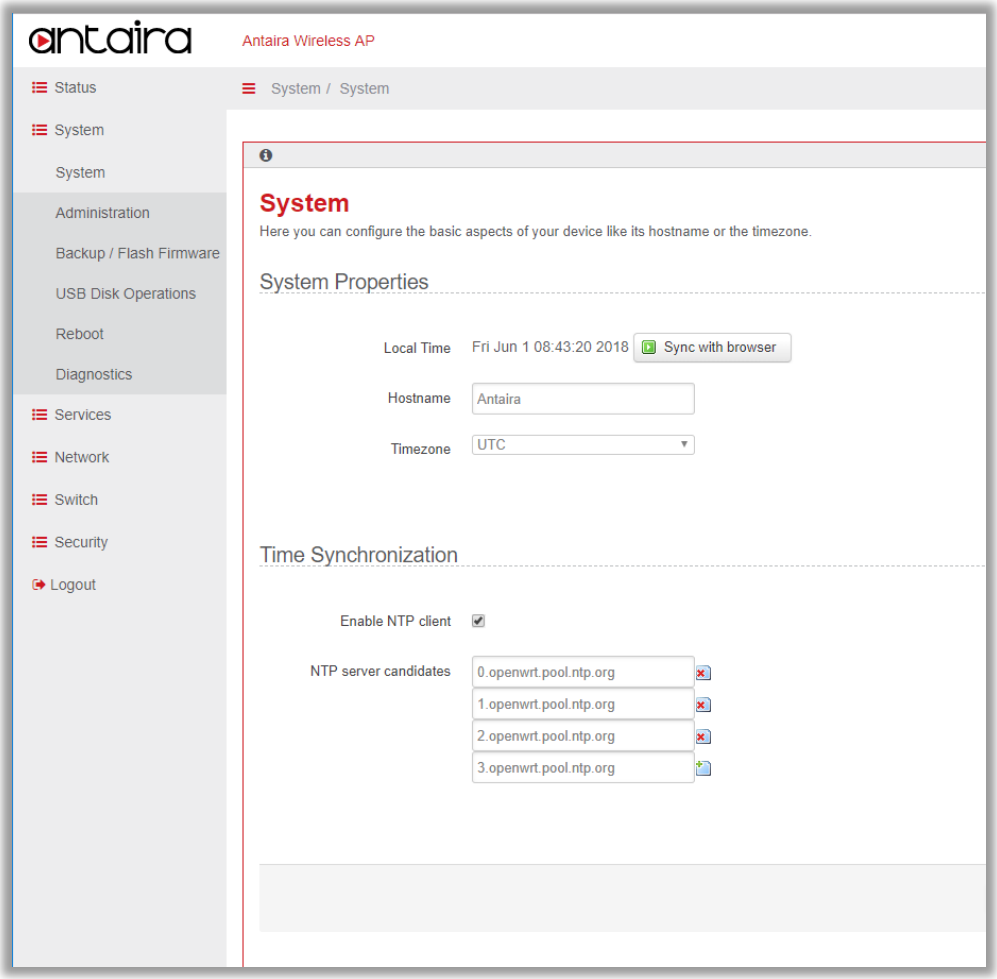
Step 3: The Web GUI can also be accessed via the Gateway's management IP address http://172.0.0.1 and the PC can be set with one IP address in the same domain 172.0.0.0.



2. System

2.1 System

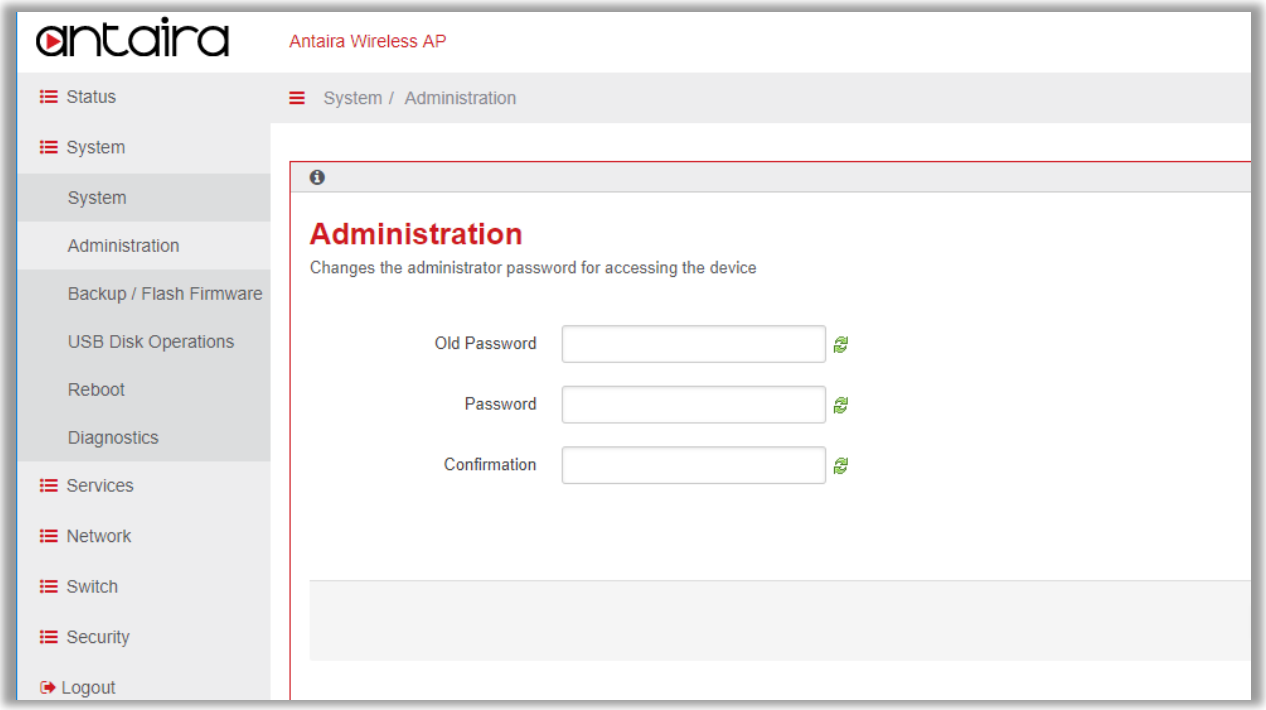
Go to **System > System** to manage the hostname and the time setting of the Antaira Wireless AP.



Item	Description
Local Time	The time status of the Antaira Wireless AP.
Hostname	Hostname of the Antaira Wireless AP.
Time zone	Time zone settings for the Antaira Wireless AP.
Enable NTP client	To enable/disable SNTP client function.
NTP server candidates	The Antaira Wireless AP will perform time synchronization with SNTP server configured here.

2.2 Administration

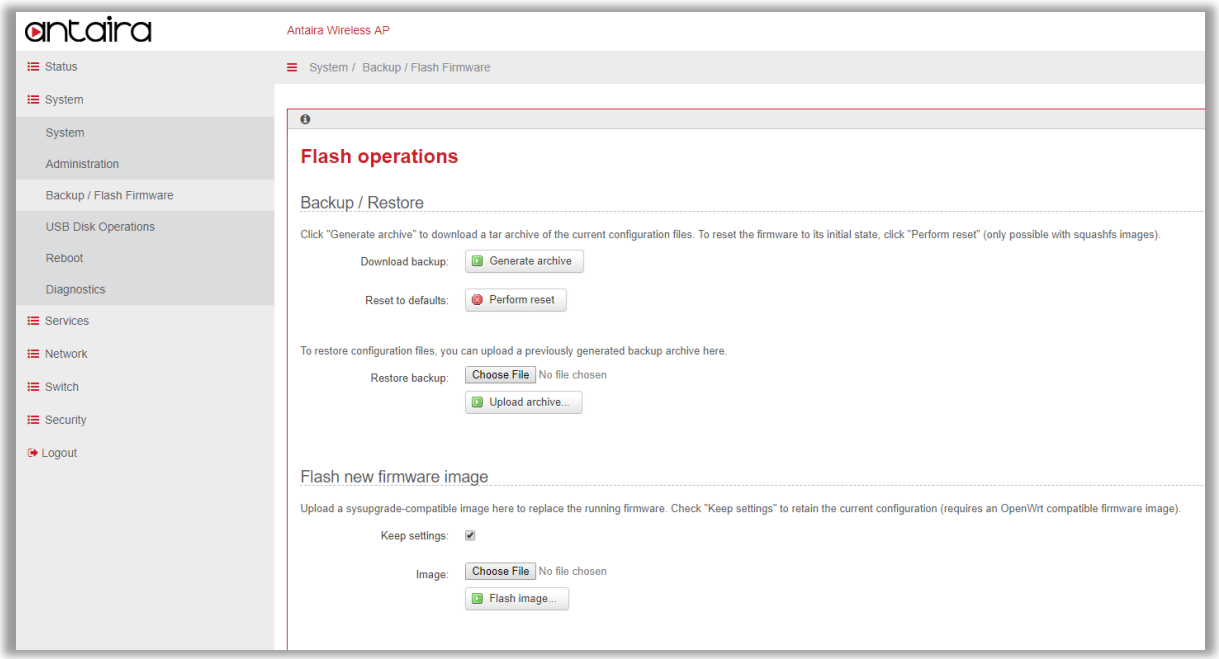
Go to **System > Administration** to change the password of Antaira Wireless AP.



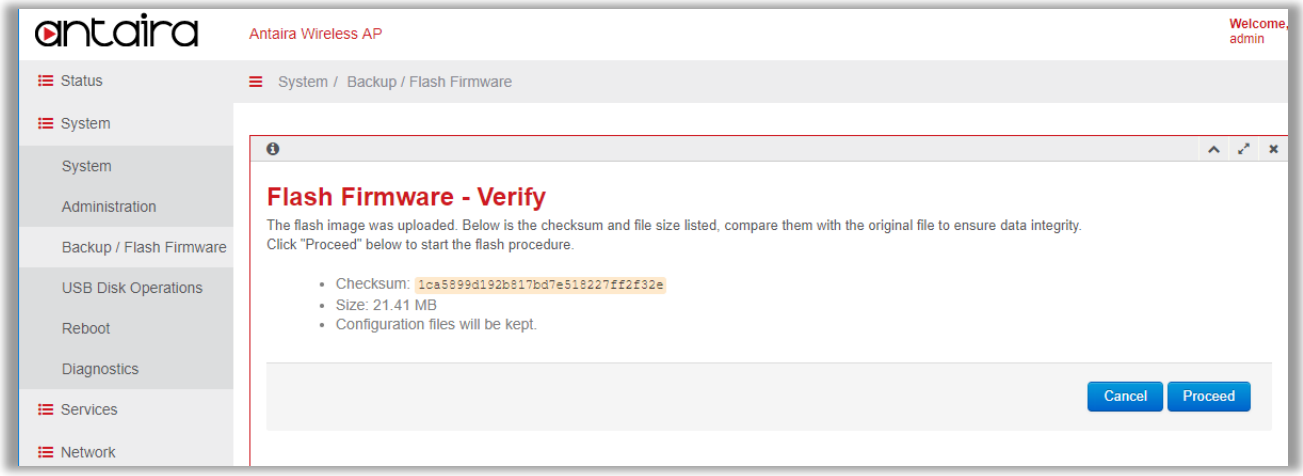
Item	Description
Old Password	Input the original password to pass the authentication of changing password.
Password	Input the new password.
Confirmation	Confirm the new password.

2.3 Backup / Flash Firmware

Go to **System > Backup / Flash Firmware** to manage the Antaira Wireless AP's configuration file and perform firmware upgrade.

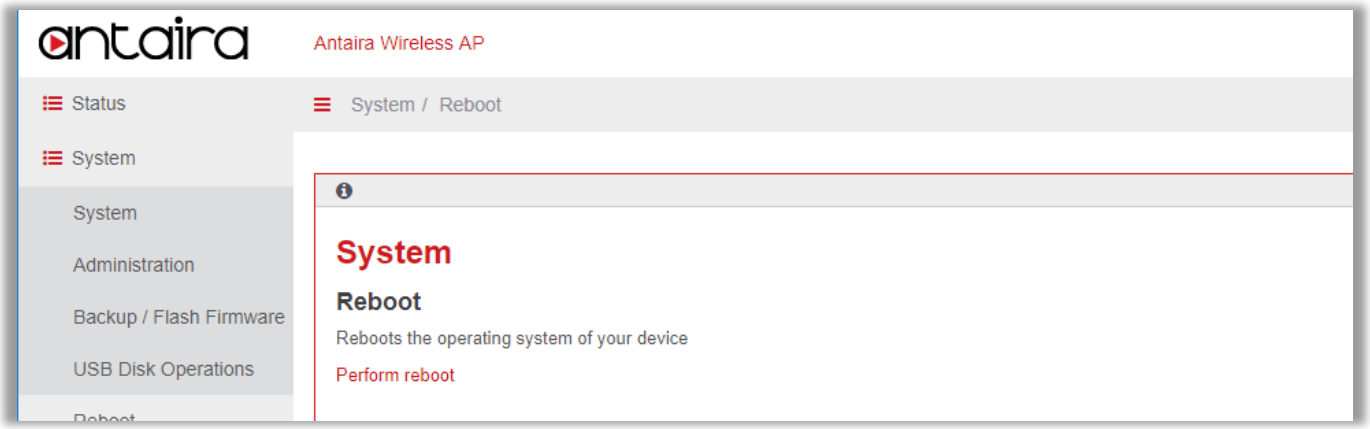


Item	Description
Generate Archive	Backup configuration file to host PC.
Perform Reset	Perform a factory reset. All configurations will be reset to factory default settings.
Upload Archive	Restore configuration file from host PC to the Antaira Wireless AP.
Keep Settings	Users can choose to only perform a firmware upgrade without resetting the configurations. It is recommended to not keep the settings due to new functions that may need to load new settings.
Flash Image	To upgrade firmware, please choose the firmware file and press **Flash Image** button.
Flash Firmware – Verify	The Antaira Wireless AP will compute the MD5 CHECKSUM for verification and ask users to proceed or cancel.



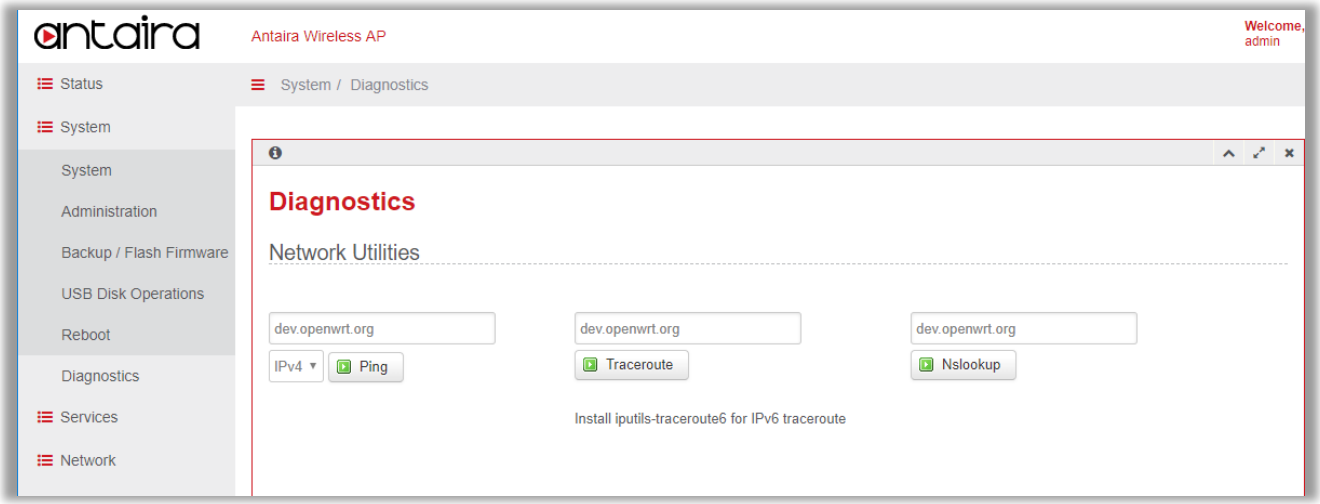
2.4 Reboot

Press **Perform reboot** link to reboot.

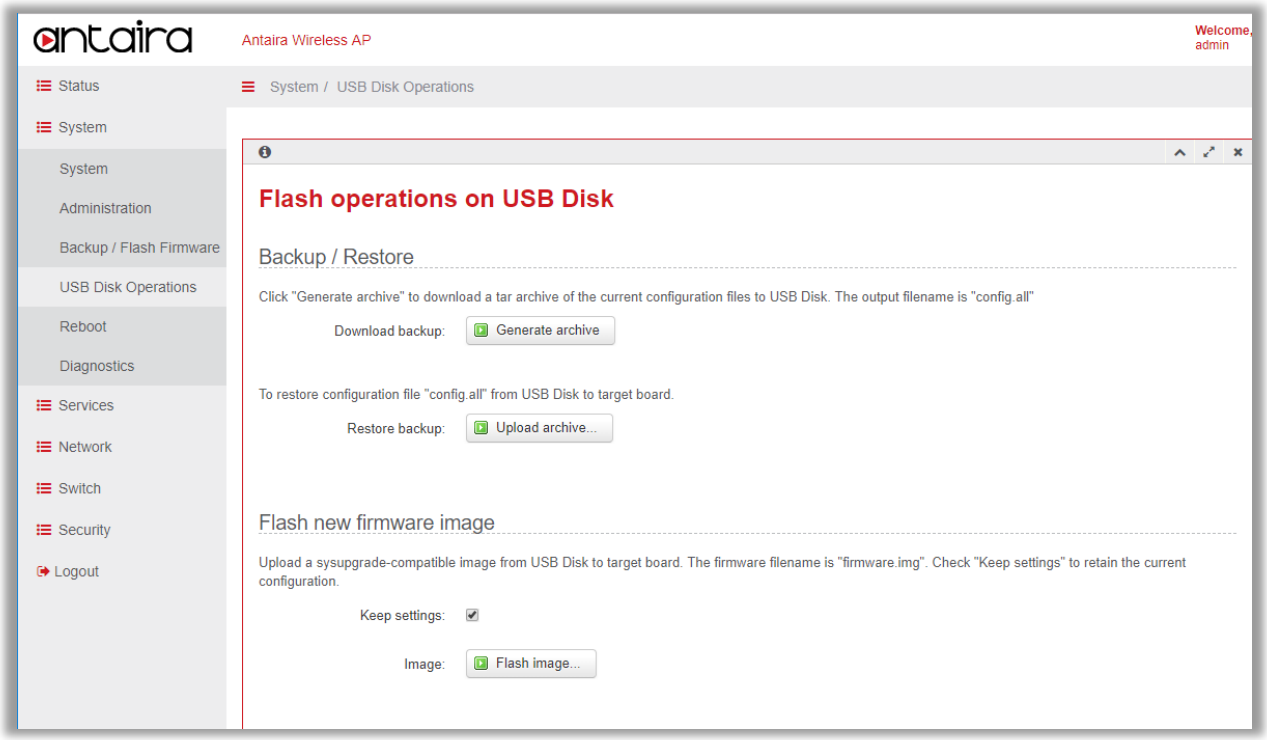


2.5 Diagnostics

Ping, Traceroute, and Nslookup Diagnostics tools.



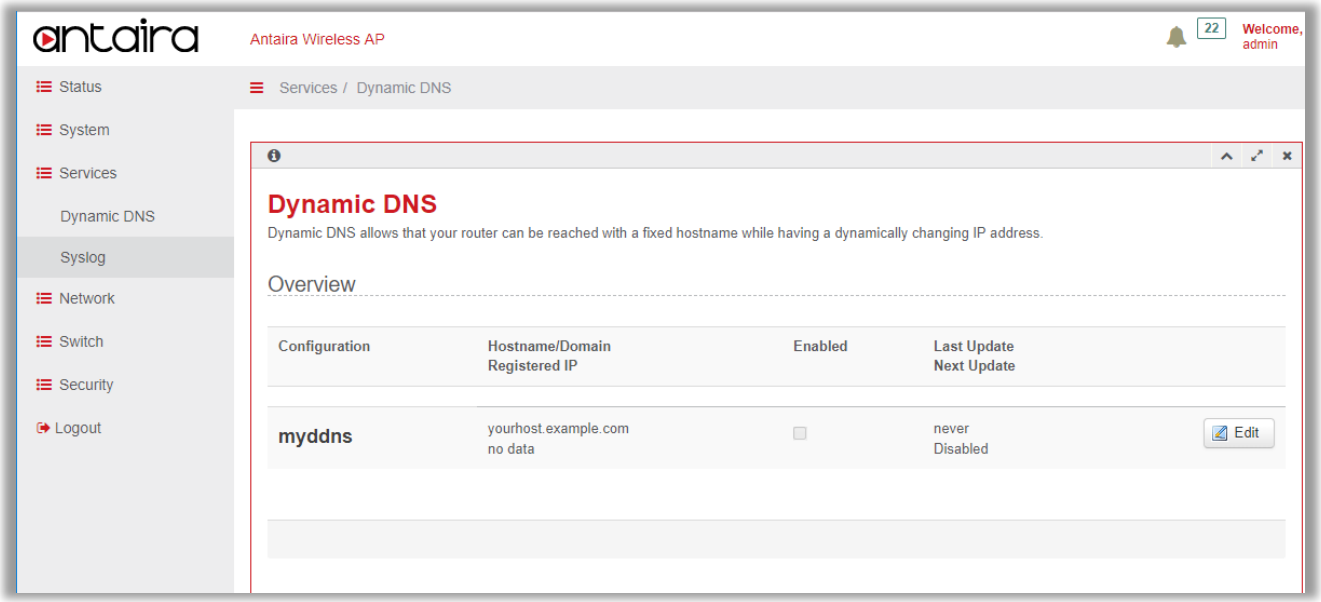
2.6 USB Disk Operation



Item	Description
Generate Archive	Backup configuration to a USB. The configuration file will be named 'config.all'.
Upload Archive	Restore configurations from USB.
Keep Settings	Users can choose to only perform a firmware upgrade without resetting the configurations. It is recommended to not keep the settings due to new functions that may need to load new settings.
Flash Image	To upgrade firmware from a USB, the firmware file needs to be named 'firmware.img'.

3. Services

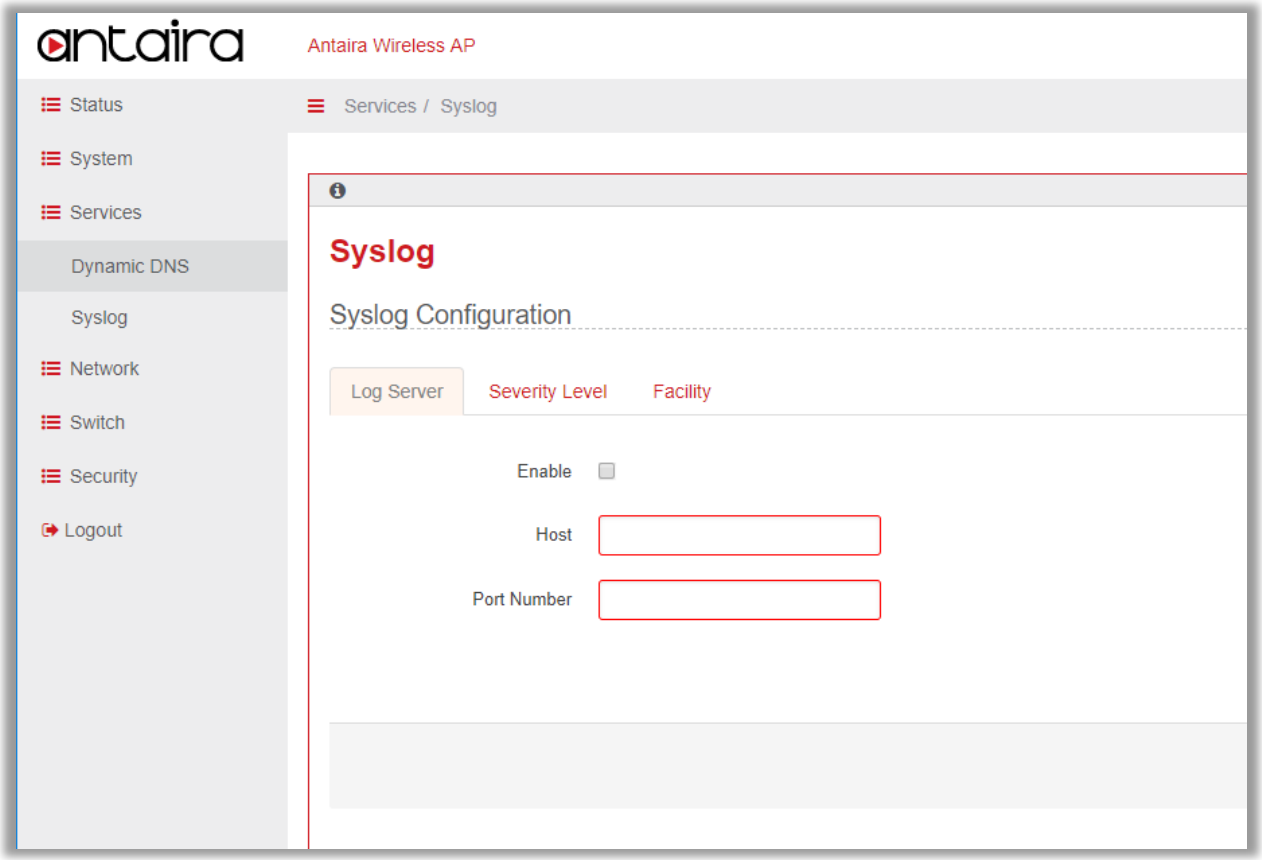
3.1 Dynamic DNS



Item	Description
Enable	To enable/disable the DDNS function.
DDNS Service Provider	To choose the DDNS provider profile.
Hostname	The hostname is used to registered to the DDNS provider for a domain name query.
Username	The username is used to registered to the DDNS provider.
Password	The password is used to registered to the DDNS provider.
Source of IP address	The source IP address used to register to the DDNS provider. (1) network: chooses an IP on specific network (2) URL: detects the current local IP from the specified website. If the Antaira Wireless AP is behind a NAT, input the WEB URL that can report the external IP address of a NAT router.
Network	User can choose an IP on WAN, LAN, or cellular interface.
URL	The correct URL might depend on the DDNS provider being used, the sample

	format should be: http://checkip.dyndns.org
Check for changed IP every and Check-time unit	A unit of time to check if the IP address is changed in the Antaira Wireless AP.
Force update every and Force-time unit	A period and unit of time for the Antaira Wireless AP to update the registered information.

3.2 Syslog



Item	Description
Enable	To enable/disable syslog sent to the remote host PC.
Host	The IP address of the remote host PC that runs syslog server.
Port Number	The port number of the remote host PC that runs syslog server.

4. Network

4.1 Network Deployment Modes

Network Deployment mode can be configured in 3 different scenarios which include '**AP'**, '**2.4GHz Client/Bridge/Repeater)**', and '**5GHz (Client/Bridge/Repeater)**'.

Modes	WAN (Ethernet)	DHCP Server @LAN/WLAN	DHCP Client @WLAN	LAN (Ethernet)	Wi-Fi 2.4GHz	Wi-Fi 5GHz
AP	O	O	X	O	AP	AP
2.4GHz (Client/Bridge/Repeater)	X	X	O	O	STA + AP	AP
5GHz (Client/Bridge/Repeater)	X	X	O	O	AP	STA + AP

Scenario	Wi-Fi 2.4GHz SSID	Wi-Fi 5GHz SSID	Remarks
AP	Antaira_2.4GHz	Antaira_5GHz	Factory Default
2.4GHz (Client/Bridge/Repeater)	Connect the uplink Root AP and broadcast the SSID which is the same as the uplink Root AP	Copy the uplink SSID and add suffix '_5GHz' over the SSID Broadcast name. i.e., XXXX_5GHz	
5GHz (Client/Bridge/Repeater)	Copy the uplink SSID and add suffix '_2GHz' over SSID Broadcast name. i.e., XXXX_2GHz	Connect the uplink Root AP and broadcast the SSID which is the same as the uplink Root AP	

4.2 Network Deployment (AP)

Network Deployment Configuration

Go to **Network > Network Deployment** and click the **Network Deployment** tab.

Network Deployment

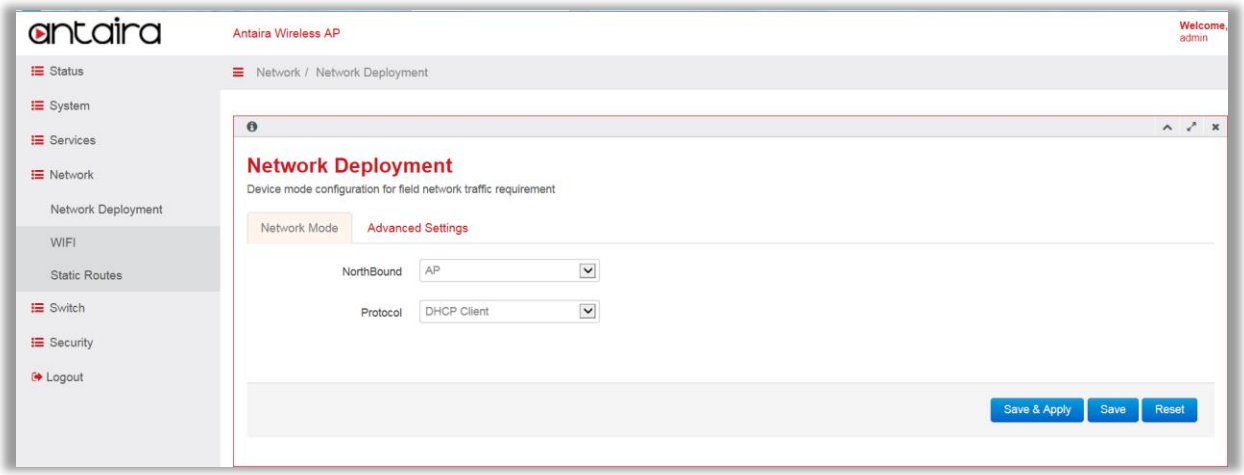
This configuration is to establish a WAN connection of the Antaira Wireless AP to the network.

Select from the Network Deployment dropdown list: **AP**.

Protocol

This protocol dropdown list will be displayed only when Network Deployment is configured to AP. It will be hidden when Network Deployment is configured to other values.

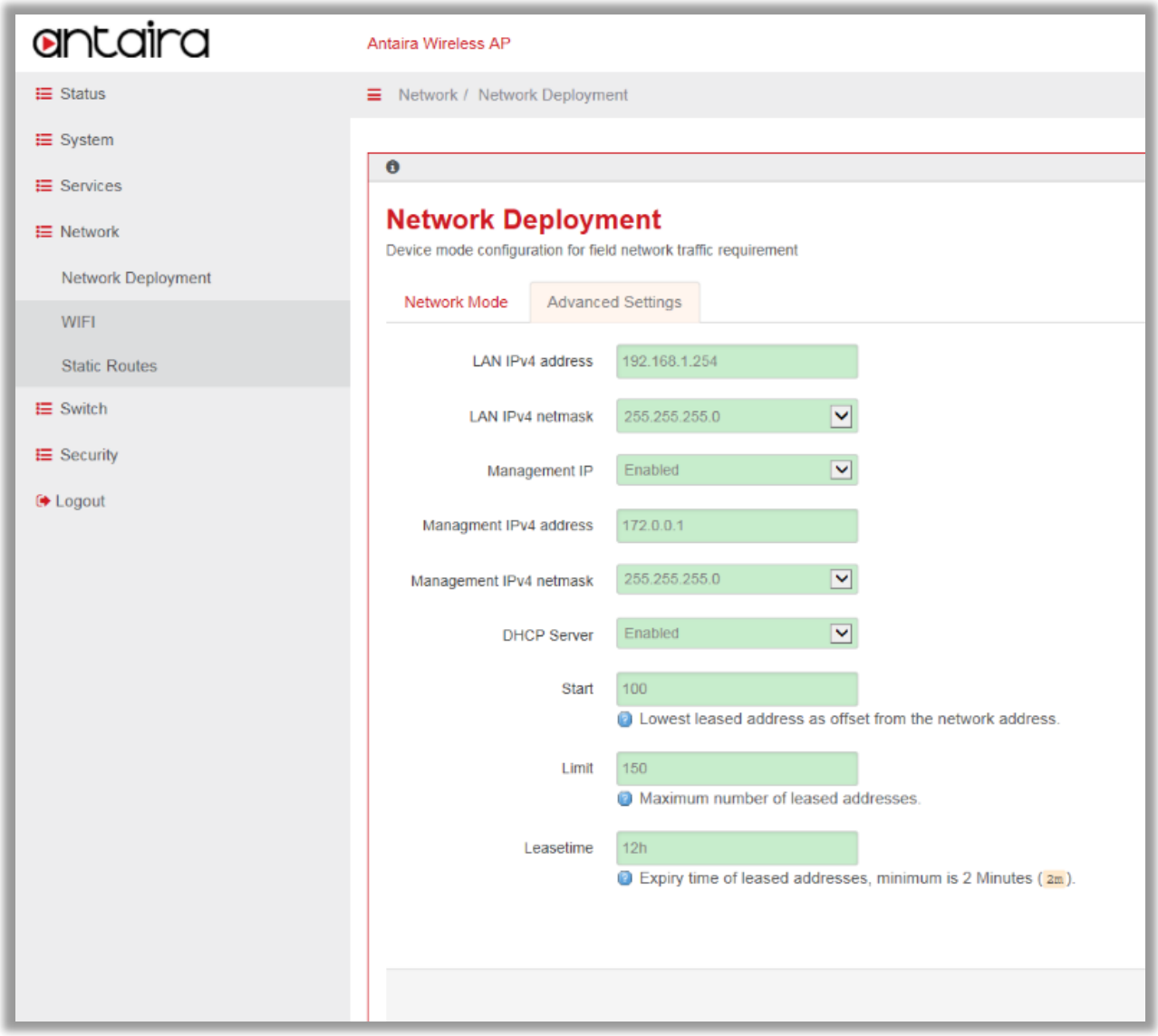
Either of the following protocol values can be selected and the device's correspondent actions, described below, are expected:


antaira
Antaira Wireless AP
Welcome, admin
Status
System
Services
Network
Network Deployment
WIFI
Static Routes
Switch
Security
Logout
Network / Network Deployment
Network Deployment
Device mode configuration for field network traffic requirement
Network Mode
Advanced Settings
NorthBound
AP
Protocol
DHCP Client
Save & Apply
Save
Reset

Item	Description
DHCP Client	Antaira's wireless AP will try to get an IP on the Ethernet WAN port via DHCP protocol.
Static IP	Antaira' wireless AP will use a static IP provided on the Ethernet WAN port. User also needs to configure the related IPv4 address, IPv4 netmask, IPv4 gateway, and DNS server.
PPPoE	Antaria's wireless AP will try to get an IP on the Ethernet WAN port via PPPoE protocol. The related PAP/CHAP username and password also needs to configured. The Access Concentrator and Service Name are optional according to the Operator's environment.

Advanced Settings Configuration

Go to **Network > Network Deployment** and click the **Advanced Settings** tab.



Item	Description
LAN IPv4 address & netmask	The Network Deployment LAN side IP address and netmask setting.
DHCP Server	The ON/OFF switch for LAN side DHCP Server function.
Start	The start of IP address that the DHCP Server will assign to the client. The lowest leased address as offset from the LAN IPv4 address (e.g. 100) or the exact start of IP address (e.g. 192.168.1.100) can be inputted.
Limit	Maximum number of leased addresses from the start of IP addresses. If user configures LAN side IP to 192.168.1/24, Start to 100 and Limit to 150. This means the IP address pool of the DHCP Server is 192.168.1.100 – 192.168.1.249.
Lease Time	Leased time of the assigned IP address from the DHCP Server.

Management IPv4 address & netmask	In the case of losing the IP address, the Web GUI can be accessed via the management IP address as well.

4.3 Network Deployment (2.4GHz WIFI)

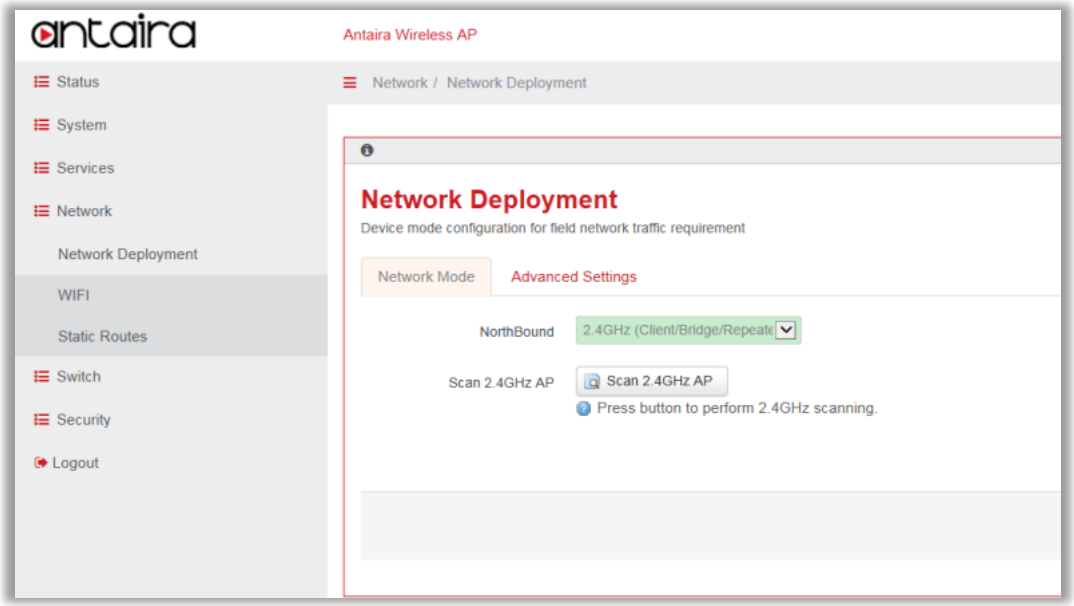
Network Deployment Configuration

Go to **Network > Network Deployment** and click the **Network Deployment** tab.

When Network Deployment is configured to 2.4GHz WIFI, Antaira Wireless AP will use 2.4GHz WIFI station to connect to the uplink AP and become a bridge AP. Thus, the clients on LAN port, 2.4GHz WIFI AP, or 5GHz WIFI AP will get an IP from uplink AP router via DHCP protocol.

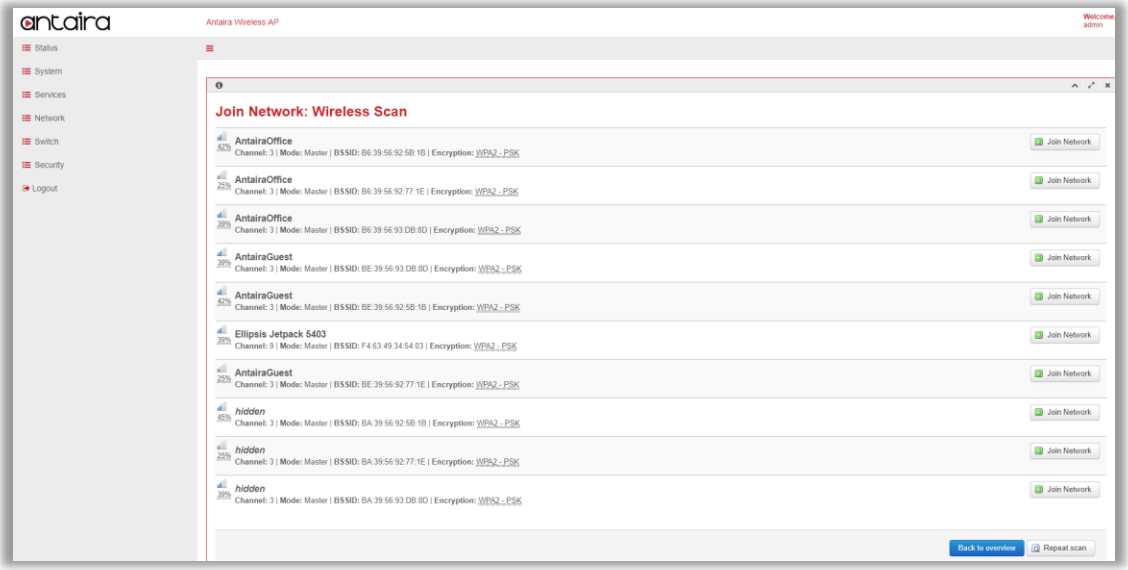
Scan 2.4GHz AP Button

This button is used to scan 2.4GHz frequency. The Antaira Wireless AP can then connect to an uplink AP router.


antaira
Antaira Wireless AP
Status
System
Services
Network
Network Deployment
WIFI
Static Routes
Switch
Security
Logout
Network / Network Deployment
Network Deployment
Device mode configuration for field network traffic requirement
Network Mode
Advanced Settings
NorthBound
2.4GHz (Client/Bridge/Repeate
Scan 2.4GHz AP
Scan 2.4GHz AP
Press button to perform 2.4GHz scanning.

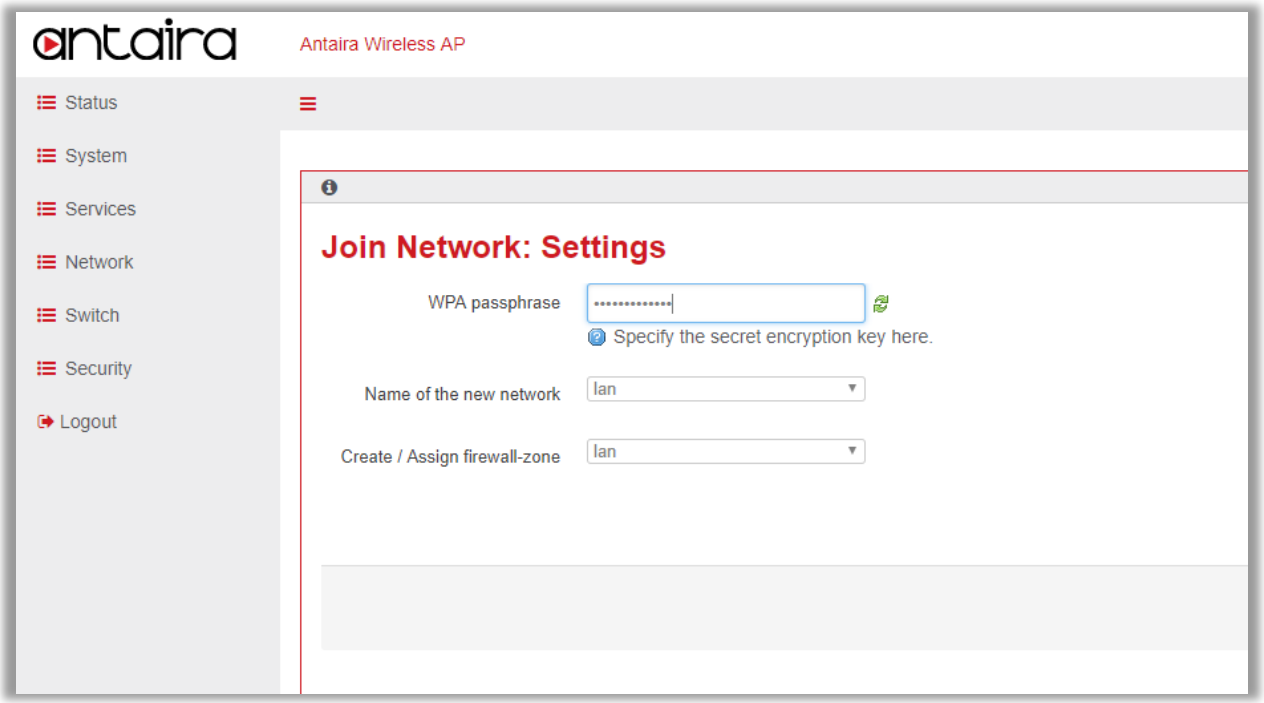
Join Network

After scanning, the specific uplink AP router can be chosen and connected to by pressing **Join Network** button.



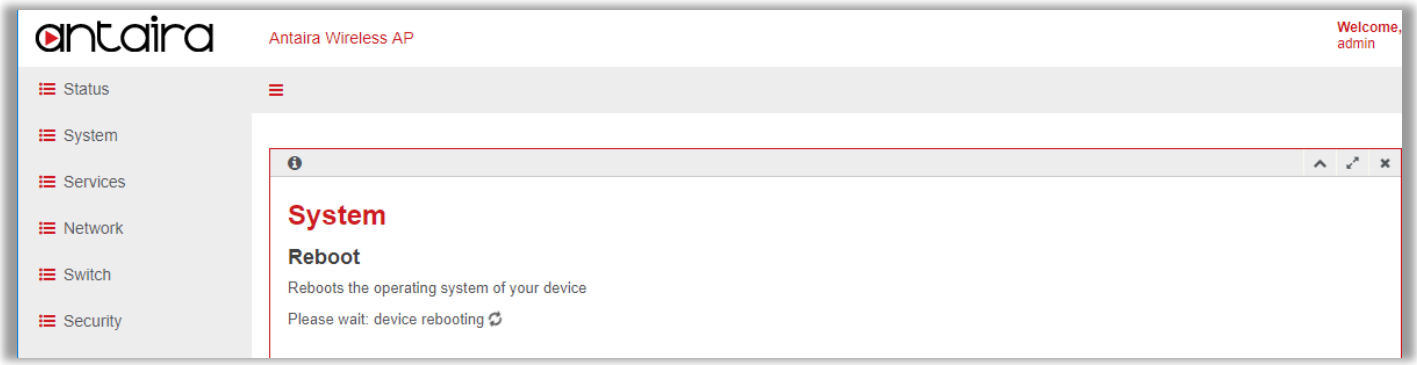
WPA passphrase

If the uplink AP router has enabled security, a WPA passphrase needs to be inputted then press **Submit**.



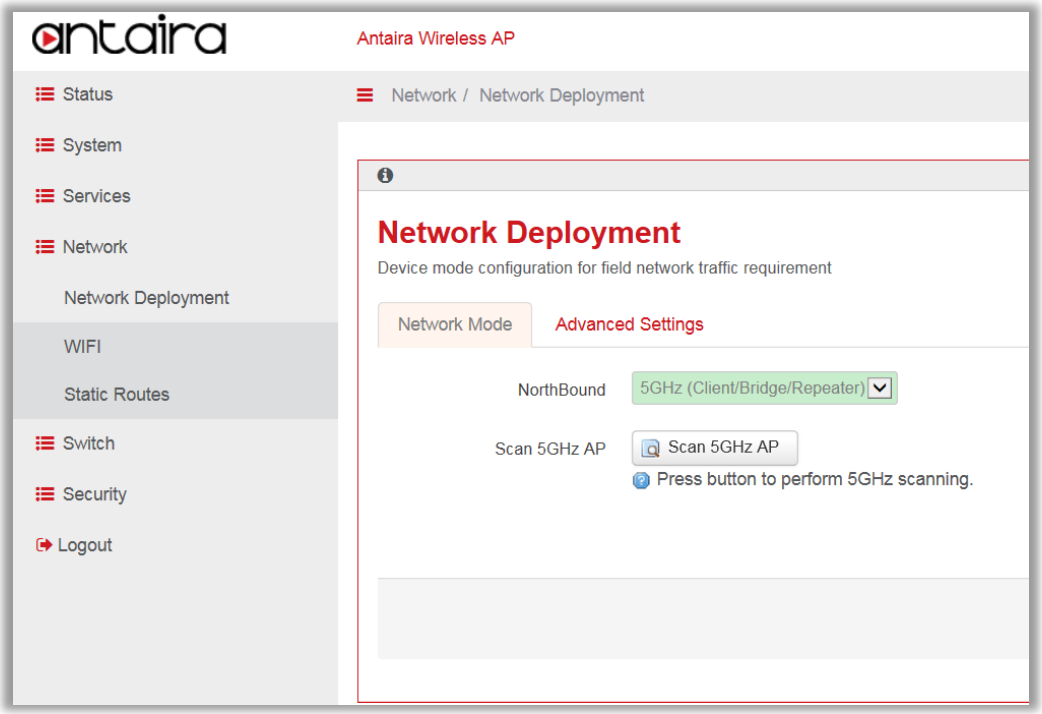
The Antaira Wireless AP will reboot automatically to allow the configurations to go into effect. When the Antaira Wireless AP boots up, it will get an IP address from the uplink AP router and LAN/WLAN side clients also need to get an IP from the uplink AP router in this mode.

4.4 Gateway Deployment (5GHz WIFI)



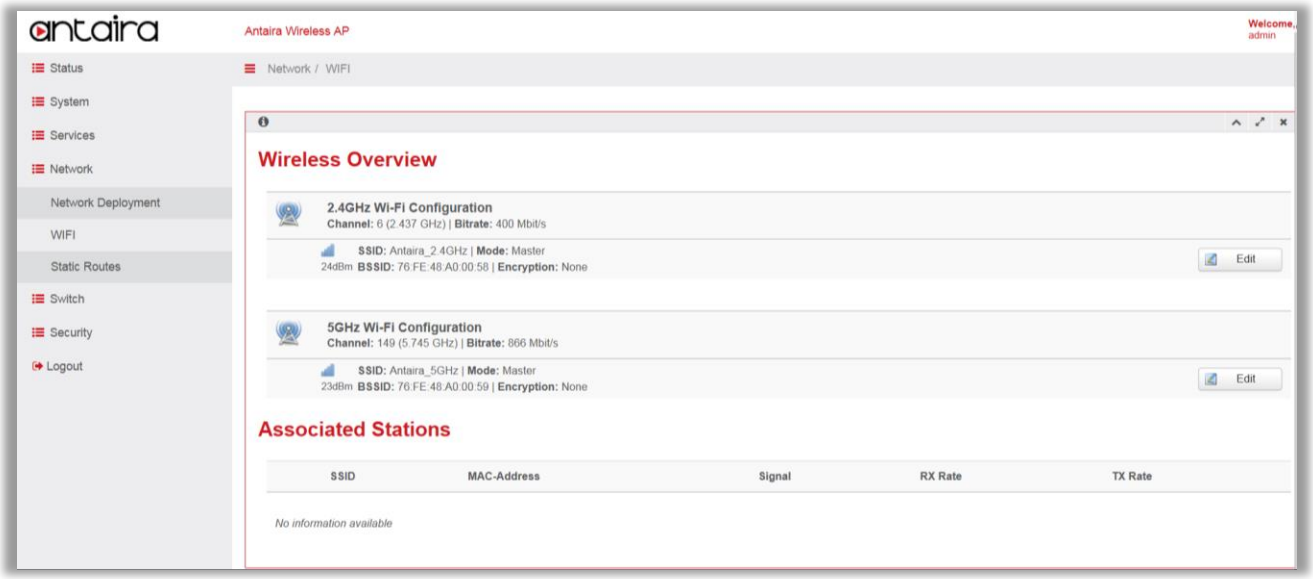
When Network Deployment is configured to 5GHz WIFI, it uses 5G WIFI station to connect to the uplink 5GHz AP. It also enables 2.4G and 5G WIFI AP simultaneously. In this mode, 5G WIFI STA, 5G WIFI AP, 2.4G WIFI AP, and Ethernet LAN are bridged together, and the device becomes an AP bridge. It uses the DHCP client to get an IP from the uplink WIFI AP router.

To connect to the uplink AP, press the **Scan 5GHz AP** button, and follow the wizard procedure. The configuration steps are the same as 2.4GHz WIFI configuration steps.



4.5 WIFI Status

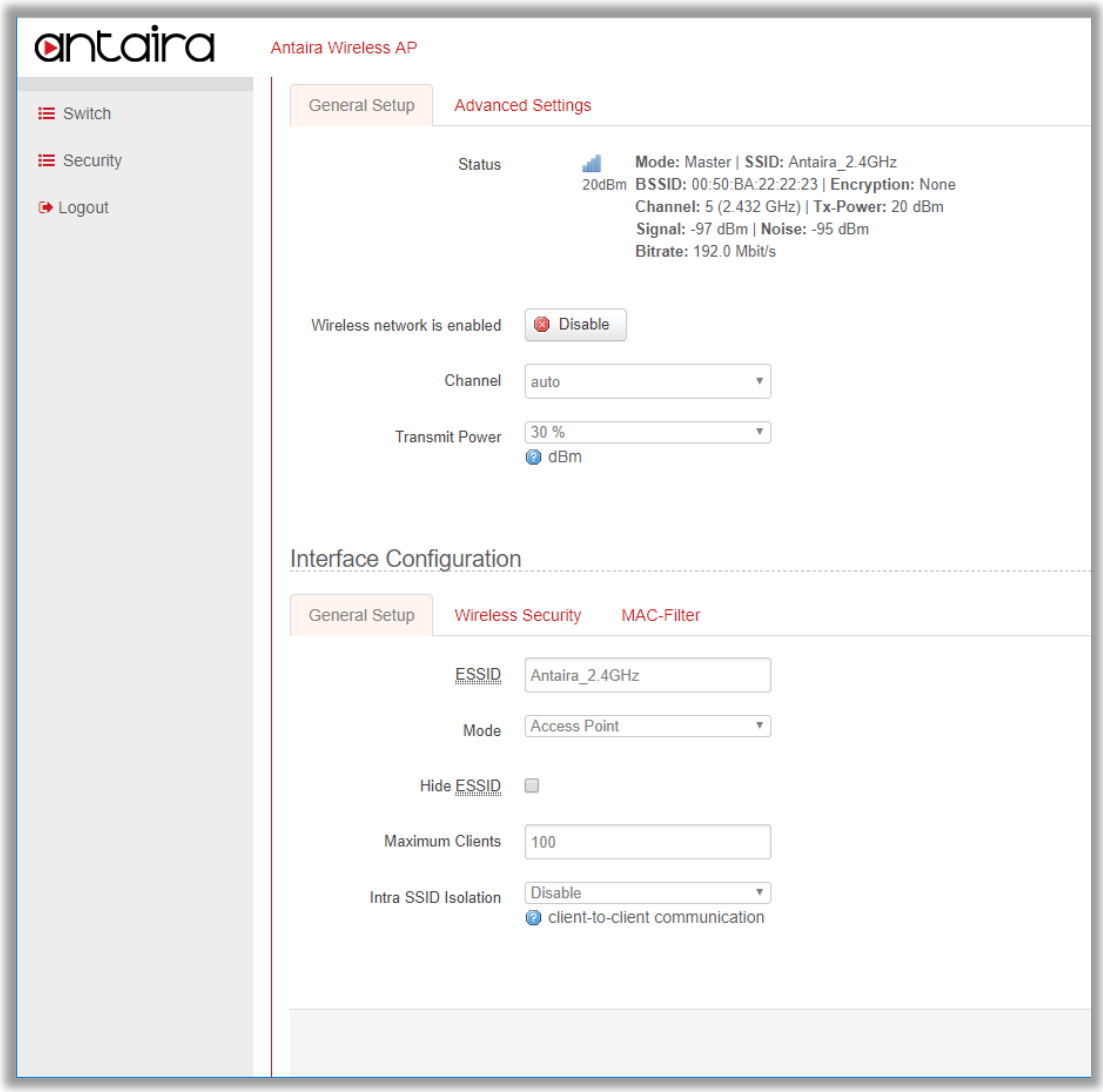
Go to **Network > WIFI** to check WIFI function status.



Item	Description
Wireless Overview	It will show 2.4GHz WIFI SSID and then 5GHz WIFI SSID. The **Edit** button can go into detail of the WIFI setting page.
Associated Stations	It will display the associated WIFI stations including 2.4GHz and 5GHz WIFI stations.

4.6 WIFI Configuration

Go to **Network > WIFI > Edit Button** to check or modify general WIFI function.

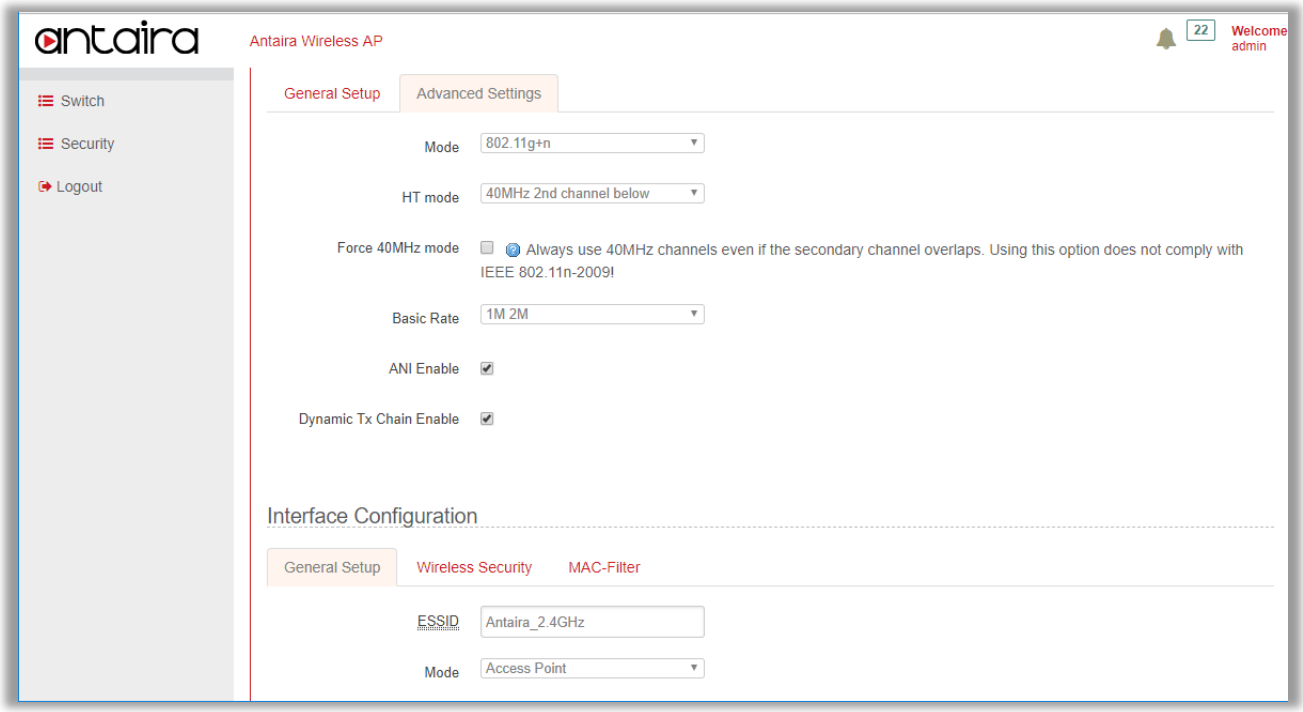


Item	Description
Wireless network is enabled	To enable/disable the WIFI SSID instance.
Channel	User can choose the desired channel or leave it as auto to automatically select.
Transmit Power	The maximum power is 20dbm mapped to 100%. The transmission power can be lowered.
ESSID	The SSID for this wireless interface.
Mode	User can configure this SSID to be AP, Client or WDS-AP, WDS-Client.

Hide ESSID	User can choose to hide SSID explored by clients.
Maximum Clients	Limit the number of clients that can connect to this SSID Instance. Default is 100.
Intra SSID Isolation	Security feature that prevents wireless clients from communicating with one another. This feature is useful for guest SSIDs by adding a level of security to limit attacks and threats between devices connected to the wireless network.

Note: If the Mode is Master, it is working as an Access Point SSID instance. If Mode is Unknown, it is working as a Station.

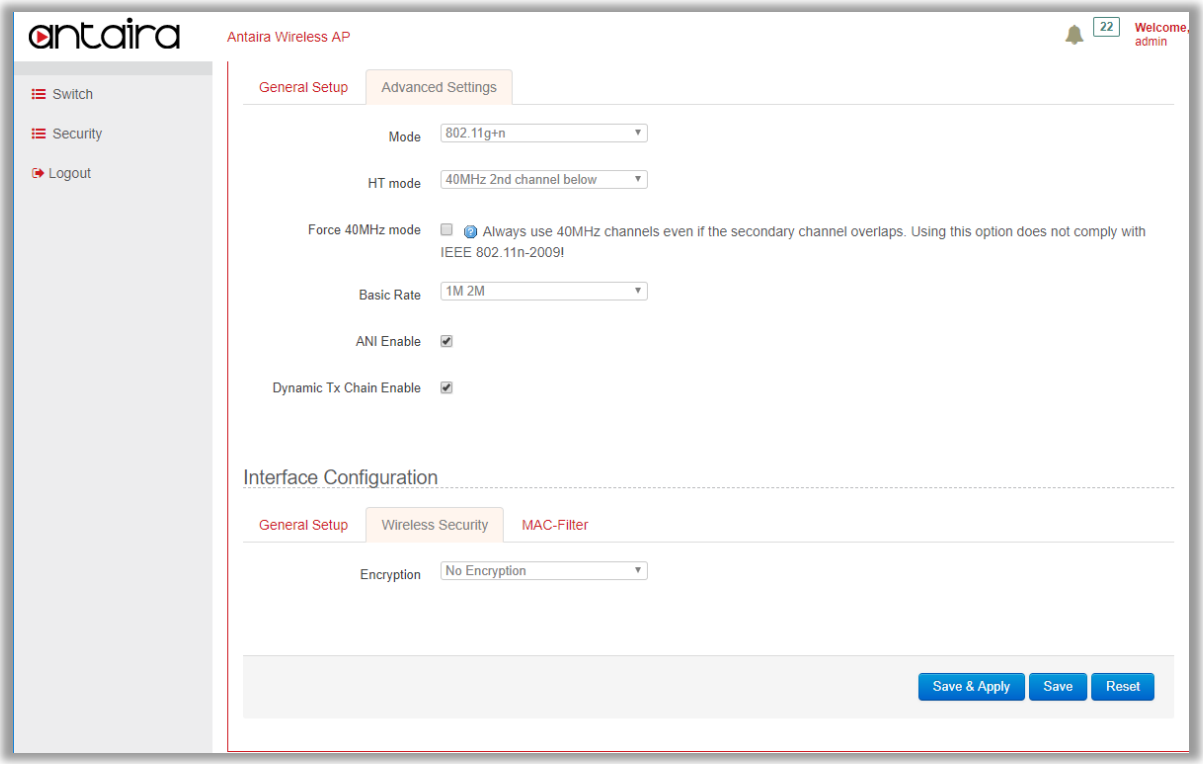
Go to **Network > WIFI > Edit Button > Device Configuration > Advanced Settings Tab** to check or modify the advance settings of device level.



Item	Description
Mode	The operating mode for the WIFI interface. It supports auto, 802.11b, 802.11g, 802.11g+n for 2.4GHz band and auto, 802.11a, 802.11a+n and 802.11ac for 5GHz band.
HT Mode	The channel bandwidth for the WIFI device. It supports 20MHz, 40MHz 2nd channel below, 40MHz 2nd channel above, and 40MHz channel for 2.4GHz band and 20MHz, 40MHz 2nd channel below, 40MHz 2nd channel above, 40MHz channel and 80MHz channel for 5GHz band
Inter SSID Isolation	WIFI station to station communication between different SSIDs.

Force 40MHz mode	Force to use 40MHz channel bandwidth. To enable it will be not compatible with IEEE 802.11n-2009, and 20MHz client cannot associate to device.
ANI Enable	To enable/disable hardware level automatically noise immunity.
Dynamic Tx Chain Enable	To enable/disable chip vendor version of efficient transmission.

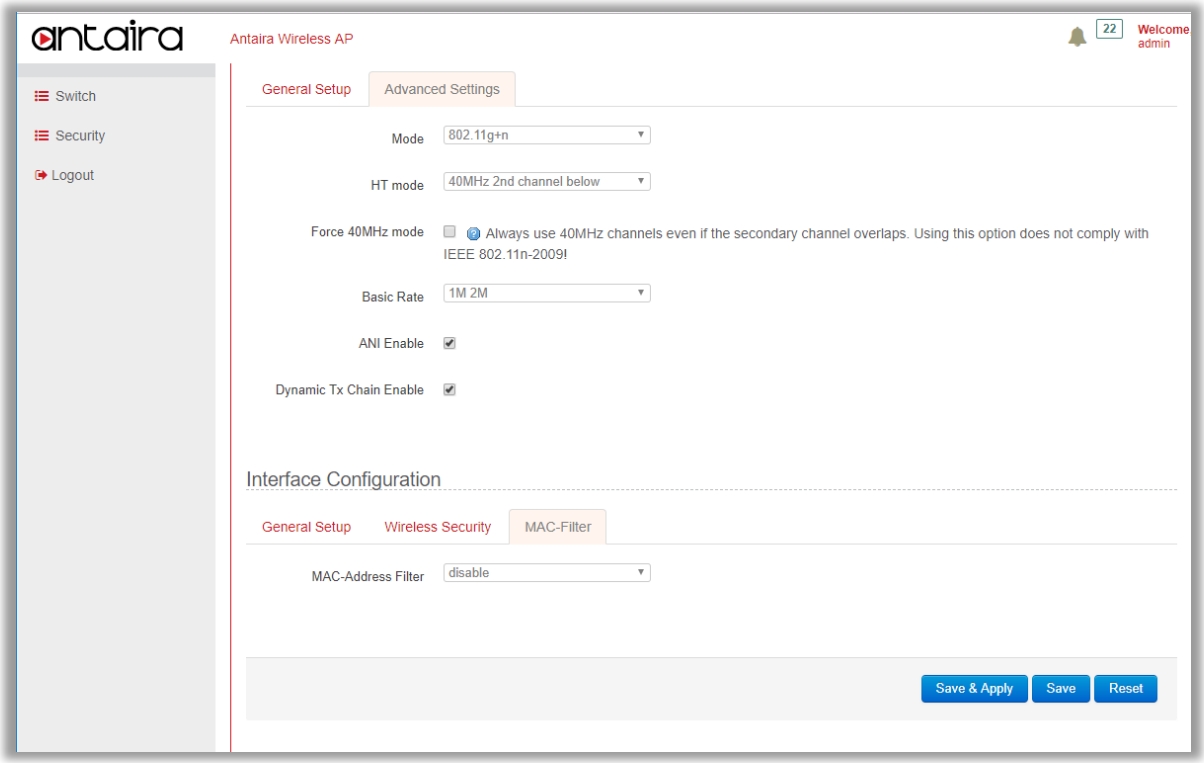
Go to **Network > WIFI > Edit Button > Interface Configuration > Wireless Security Tab** to check or modify security settings of interface level.



Item	Description
Encryption	The WIFI security settings. It supports No Encryption, WEP Open System, WEP Shared Key, WEP Mixed, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode, WPA-EAP, and WPA2-EAP.
Used Key Slot / Key#1 / Key#2 / Key#3 / Key#4	The security sub items when WEP is chosen. The Used Key Slot indicates which key is used for encryption. Four keys can be introduced in system.
Cipher / Key	The Cipher method and Key value for WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK Mixed Mode. The Cipher method supports auto, Force CCMP(AES), Force TKIP, Force TKIP, and CCMP(AES).
Cipher / Radius-	The RADIUS configuration for WPA-EAP and WPA2-EAP. The authentication

Authentication-Server(/Port/Secret) / Radius-Account-Enable / NAS ID	and accounting will be performed on RADIUS server, and the Antaira Wireless AP works as authenticator.
ANI Enable	To enable/disable hardware level automatically noise immunity.
Dynamic Tx Chain Enable	To enable/disable chip vendor version of efficient transmission.

Go to **Network > WIFI > Edit Button > Interface Configuration > MAC Filter Tab** to check or modify the WIFI station MAC filter settings of interface level.


antaira
Antaira Wireless AP
22
Welcome
admin
Switch
Security
Logout
General Setup
Advanced Settings
Mode
802.11g+n
HT mode
40MHz 2nd channel below
Force 40MHz mode
Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!
Basic Rate
1M 2M
ANI Enable
Dynamic Tx Chain Enable
Interface Configuration
General Setup
Wireless Security
MAC-Filter
MAC-Address Filter
disable
Save & Apply
Save
Reset

Item	Description
MAC-Address Filter	This is the chip level MAC filter used to drop station traffic. It supports Allow listed only (white list) and Allow all except listed (black list).
MAC-List	To input the MAC address of station to deny.

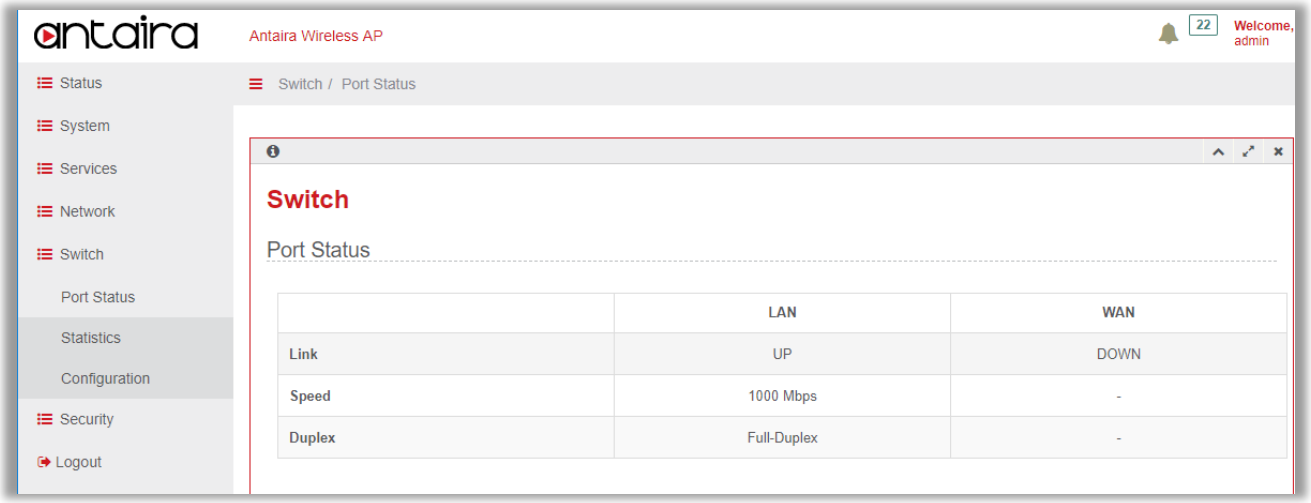
4.7 Static Routes

Go to **Network > Static Routes** to manage static route of Antaira Wireless AP. User can add host route or network route according to deployment environment.

5. Switch

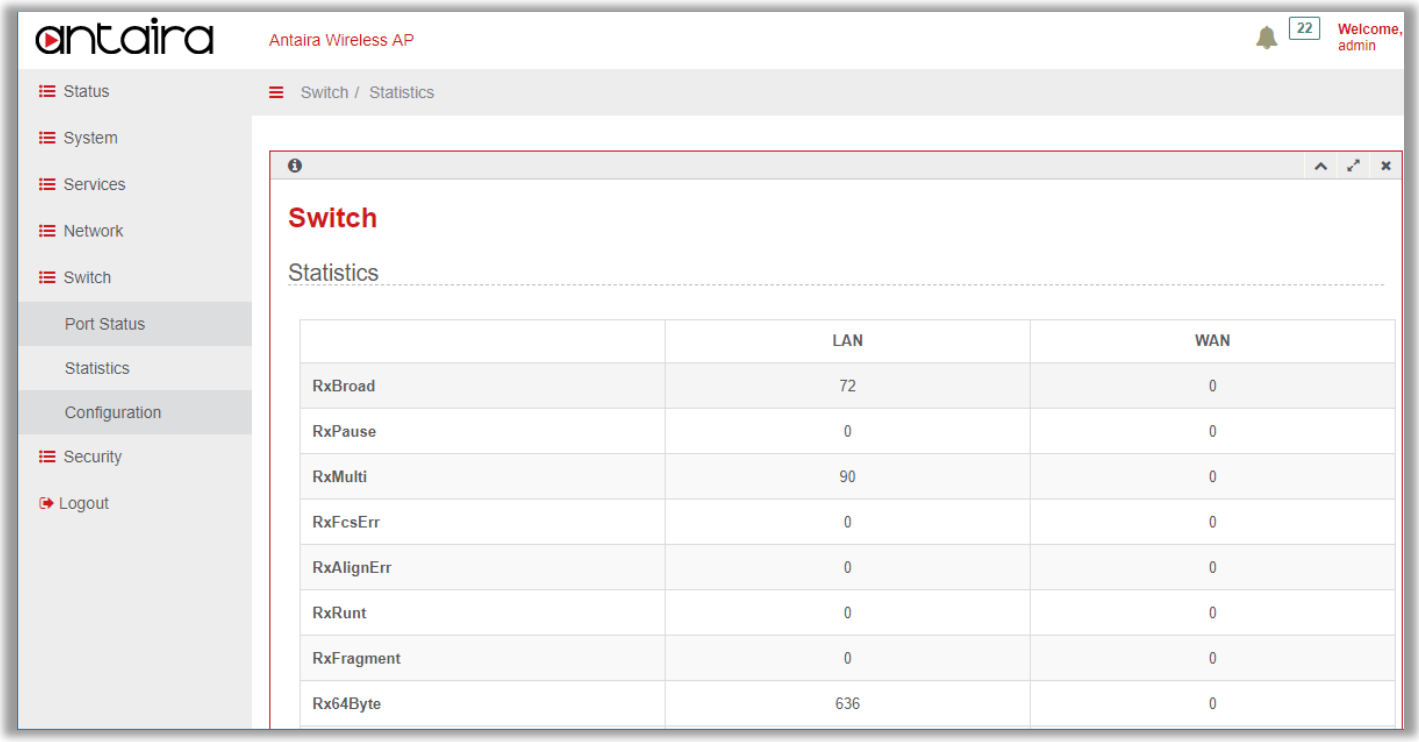
5.1 Port Status

Go to **Switch > Port Status** to check the LAN and WAN link statuses.



5.2 Statistics

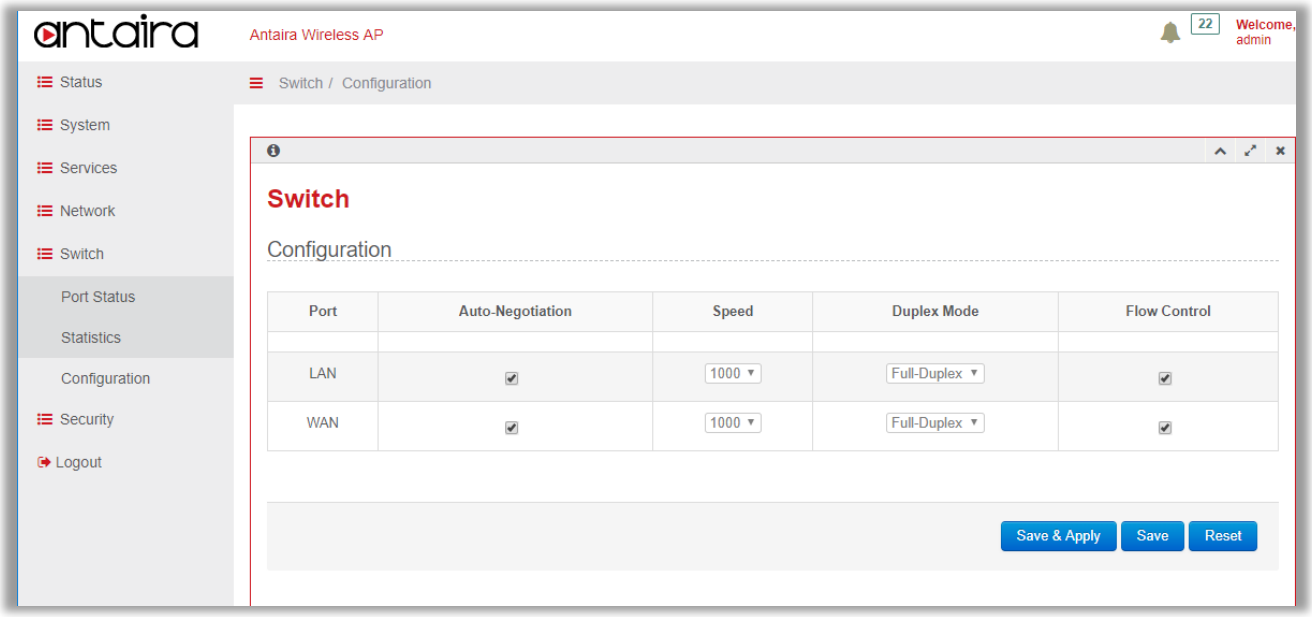
Go to **Switch > Statistics** to check the LAN and WAN switch port counter statuses.



	LAN	WAN
RxBroad	72	0
RxPause	0	0
RxMulti	90	0
RxFcsErr	0	0
RxAlignErr	0	0
RxRunt	0	0
RxFragment	0	0
Rx64Byte	636	0

5.3 Configuration

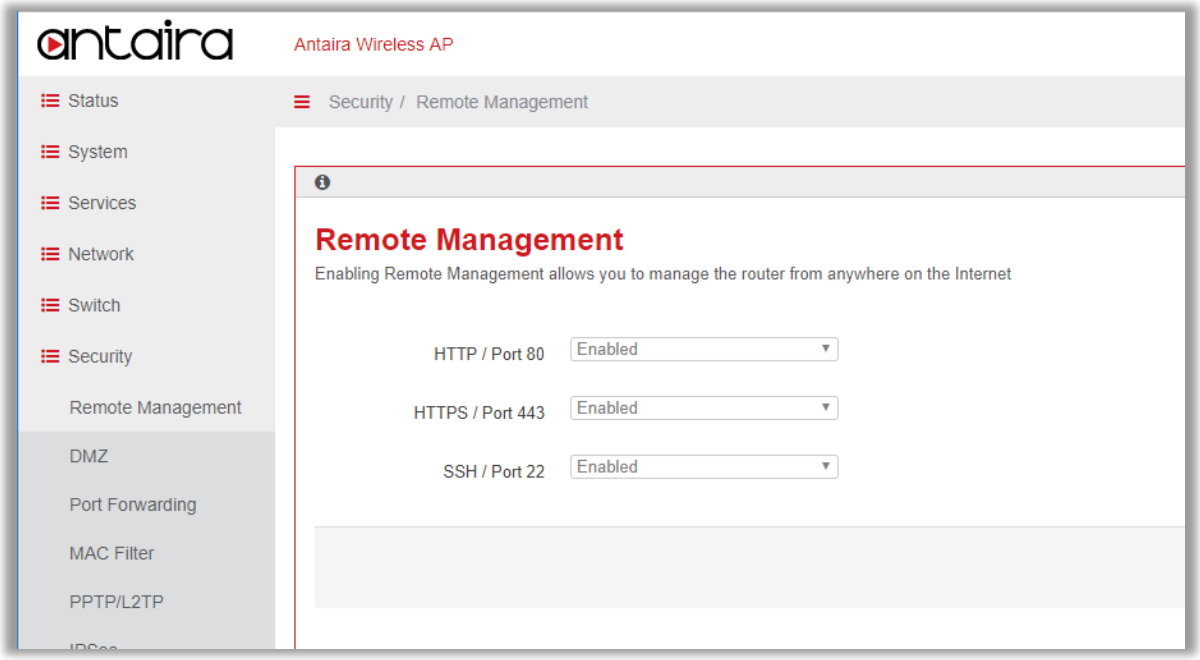
Go to **Switch > Configuration** to manage the LAN and WAN switch port configurations. User can enable/disable **Auto-Negotiation**, **Speed**, **Duplex Mode** and **Flow Control** according the deployment environment.



6. Security

6.1 Remote Management

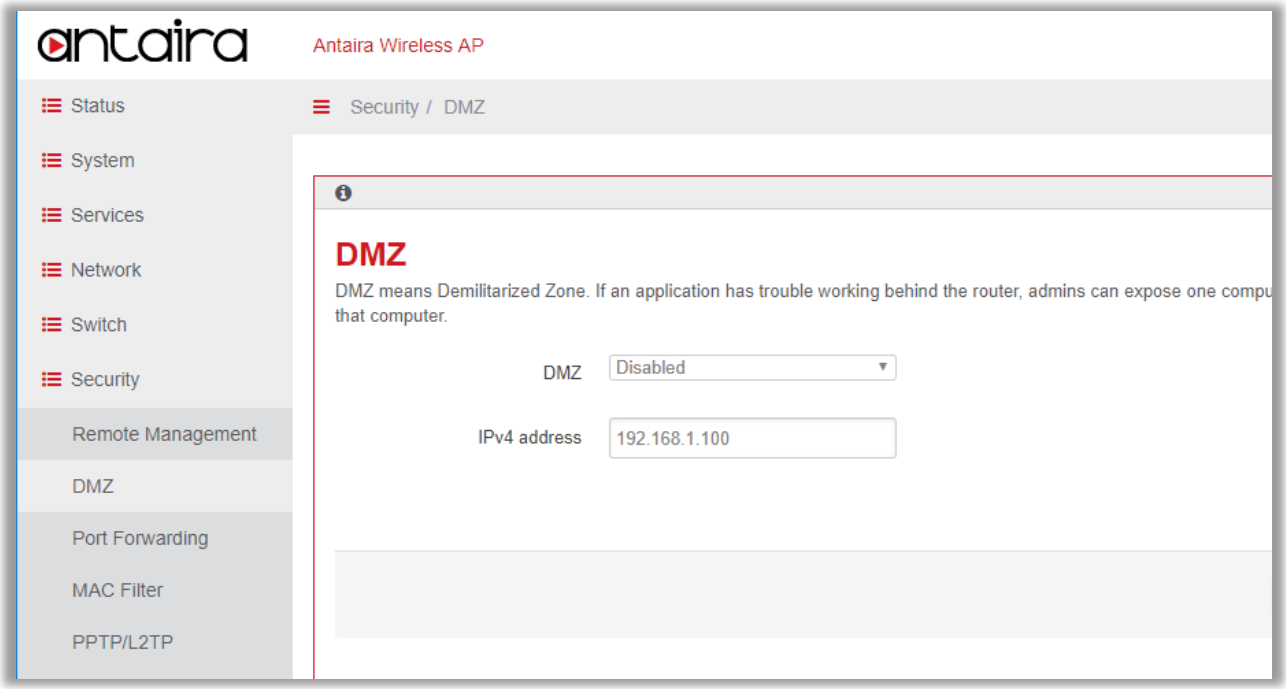
Go to **Security > Remote Management** to open port on WAN zone interface.



Item	Description
HTTP / Port 80, HTTPS / Port 443 SSH / Port 22	To enable/disable port access from the WAN zone interface. The WAN zone interfaces include Ethernet WAN and 3G module. After enabling the port on the WAN zone interface, an external host can access related services running on the Antaira Wireless AP.

6.2 DMZ

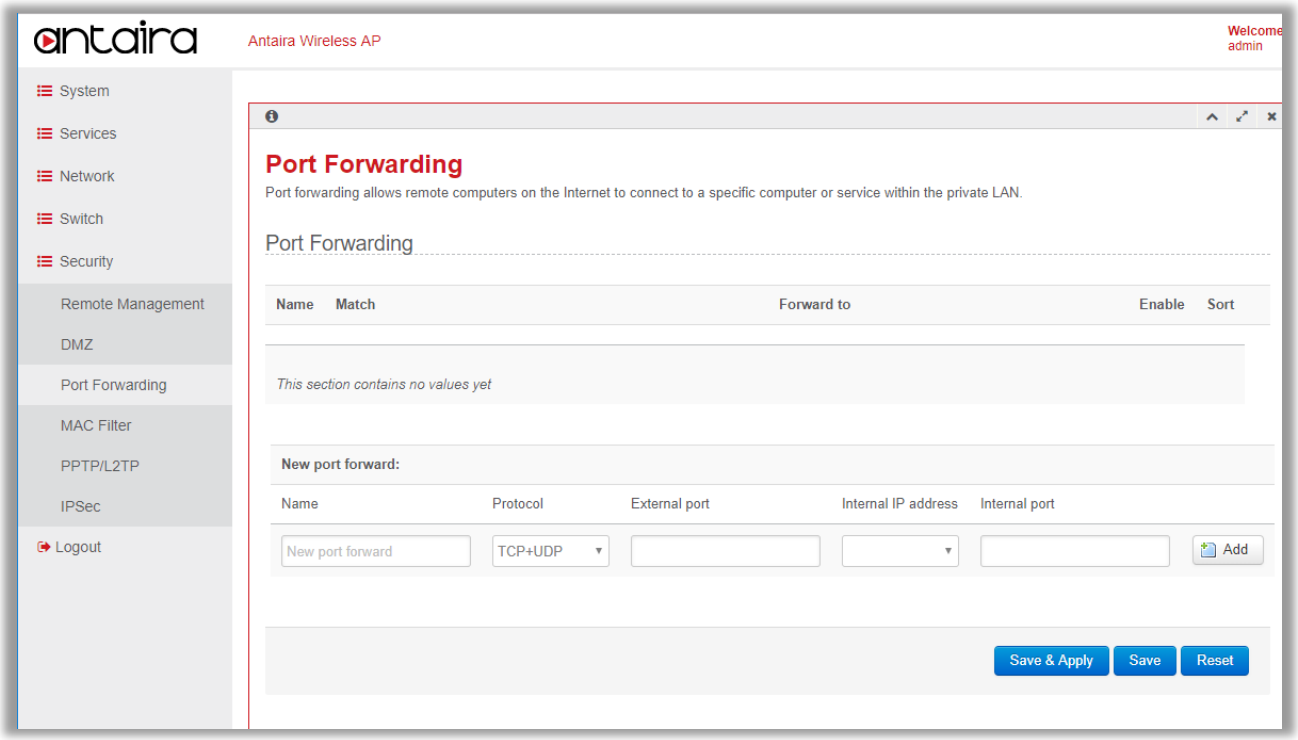
Go to **Security > DMZ** to enable/disable DMZ function.



Item	Description
DMZ	To enable/disable DMZ function.
IPv4 Address	When DMZ is enabled, all traffic that comes to the port of WAN zone will be forwarded to this private host.

6.3 Port Forwarding

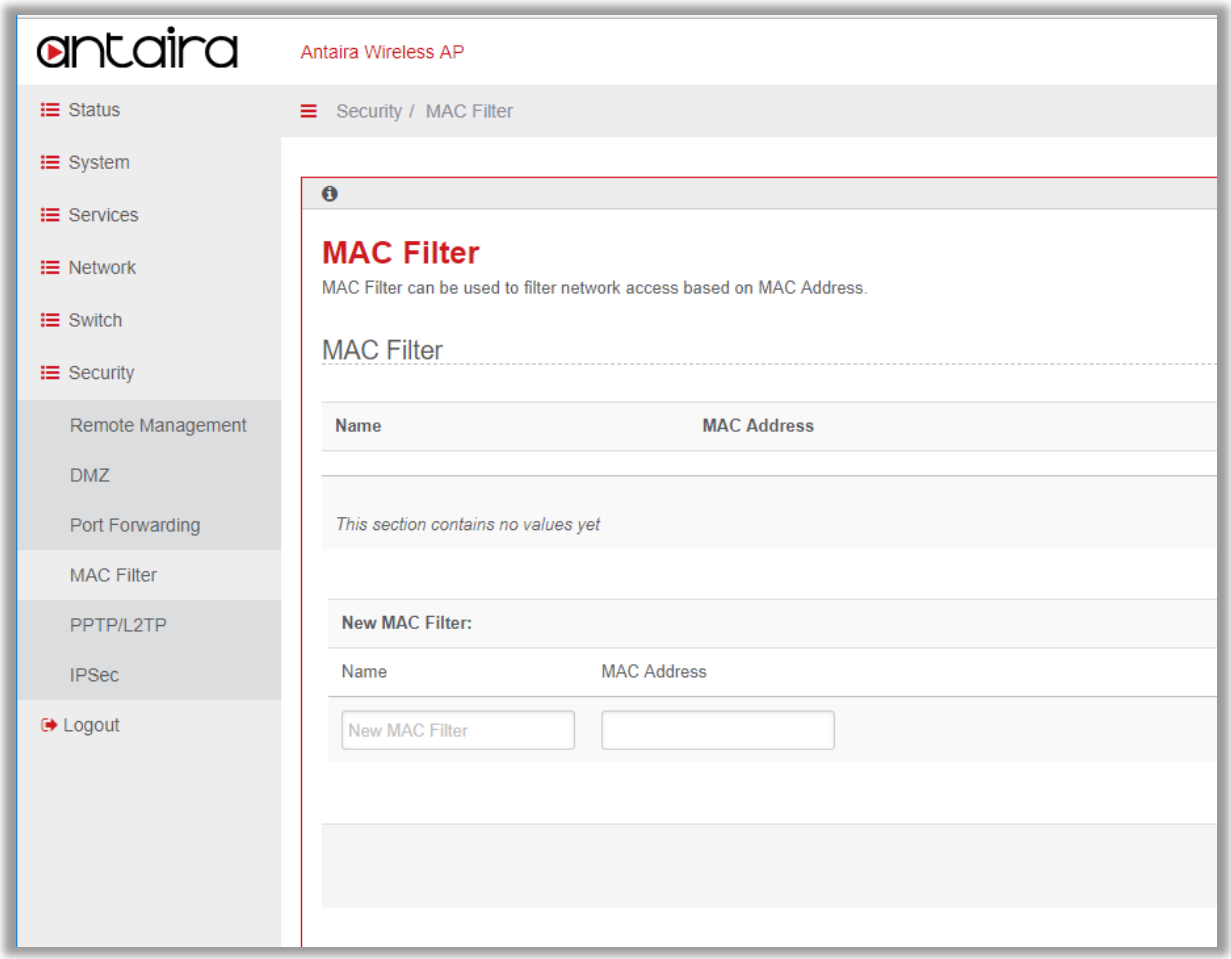
Go to **Security > Port Forwarding** to add/delete port forwarding rule.



Item	Description
Port Forwarding	One port forwarding rule includes Rule Name, Protocol, External Port, Internal IP Address, and Internal Port fields. Port Forwarding allow specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for a number of applications such as FTP servers, Web servers, e-mail servers, etc. Port Forwarding is also beneficial where different host systems need to be seen using a single common IP address/port.

6.4 MAC Filter

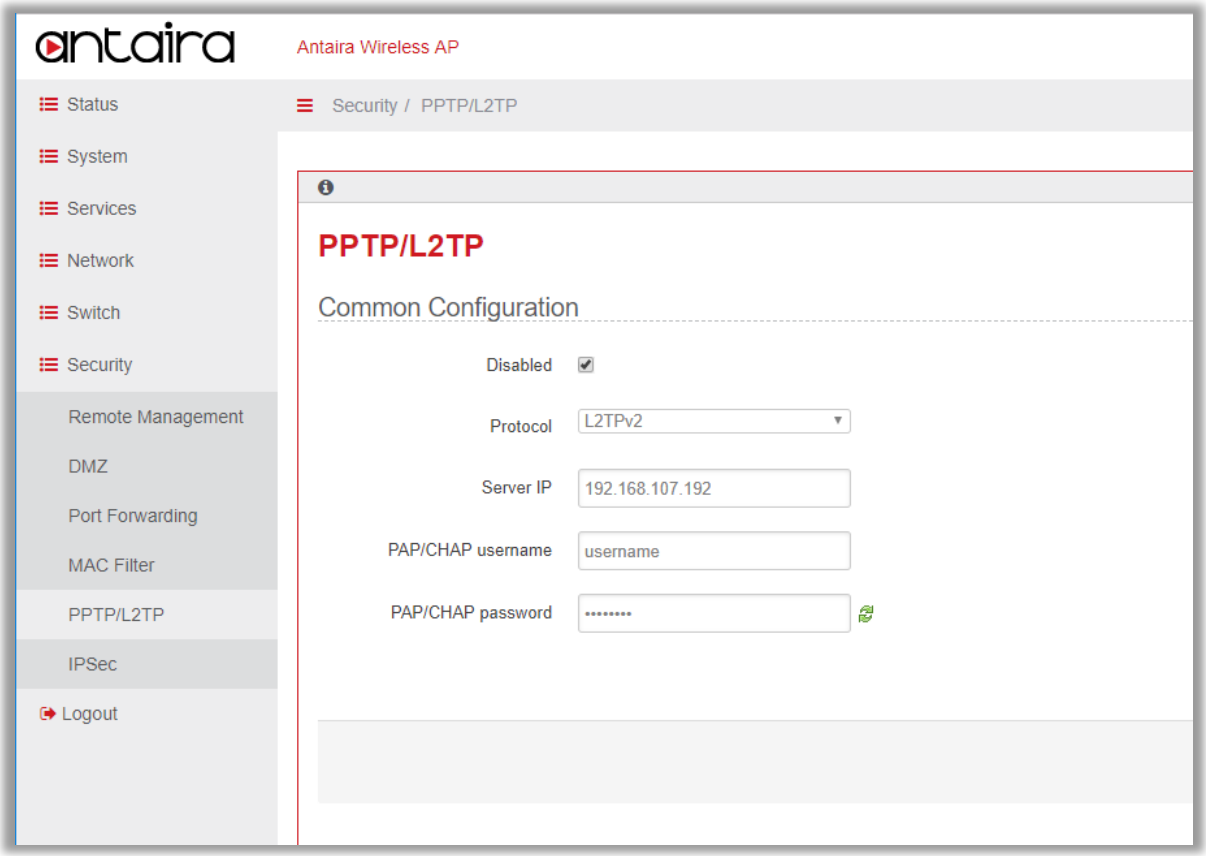
Go to **Security > MAC filter** to add/delete MAC filter rule.



Item	Description
MAC Filter	One MAC Filter rule includes Rule Name and MAC Address. This function is to drop packets with the configured source MAC Address.

6.5 PPTP/L2TP

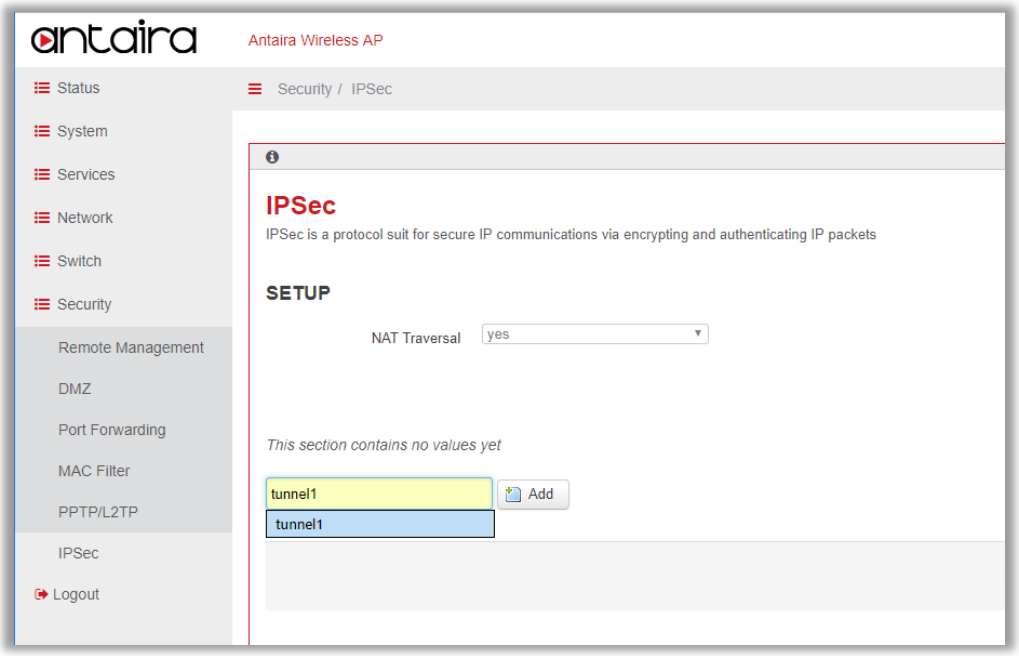
Go to **Security > PPTP/L2TP** to enable/disable PPTP/L2TP function.



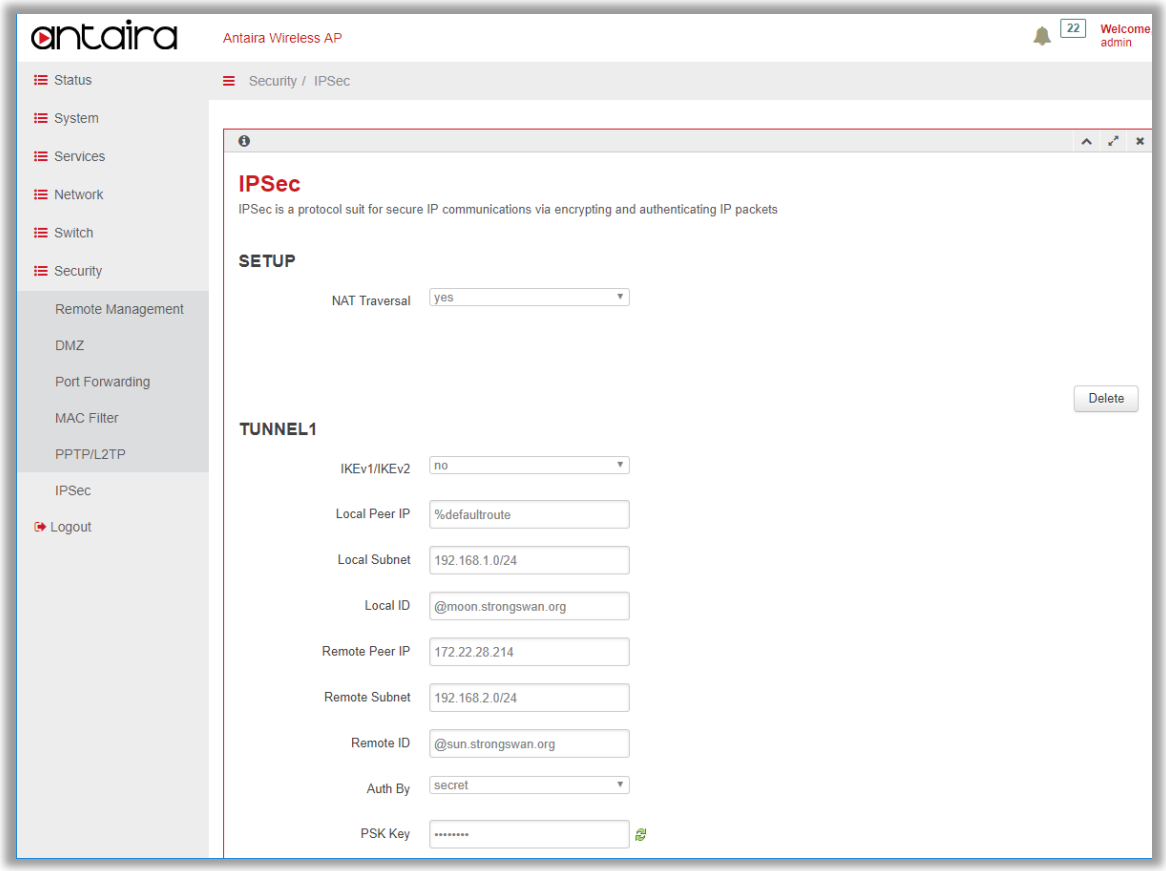
Item	Description
Disabled	By default, PPTP/L2TP are disabled. To enable PPTP/L2TP, uncheck this item.
Protocol	Choose between PPTP or L2TP.
Server IP	The PPTP/L2TP server to connect to.
PAP/CHAP username & password	The account login information to the PPTP/L2TP server.

6.6 IPSec

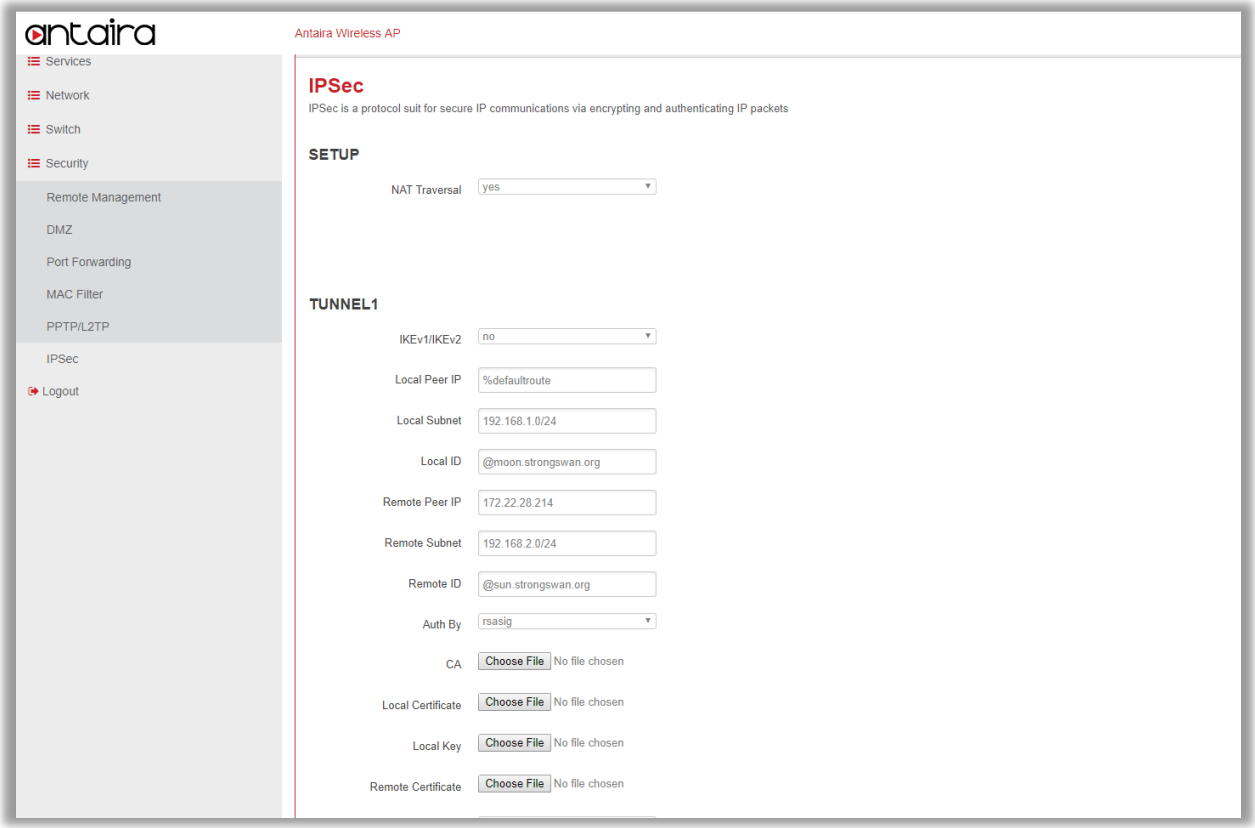
Go to **Security > IPSec** to configure IPSec tunnel settings.



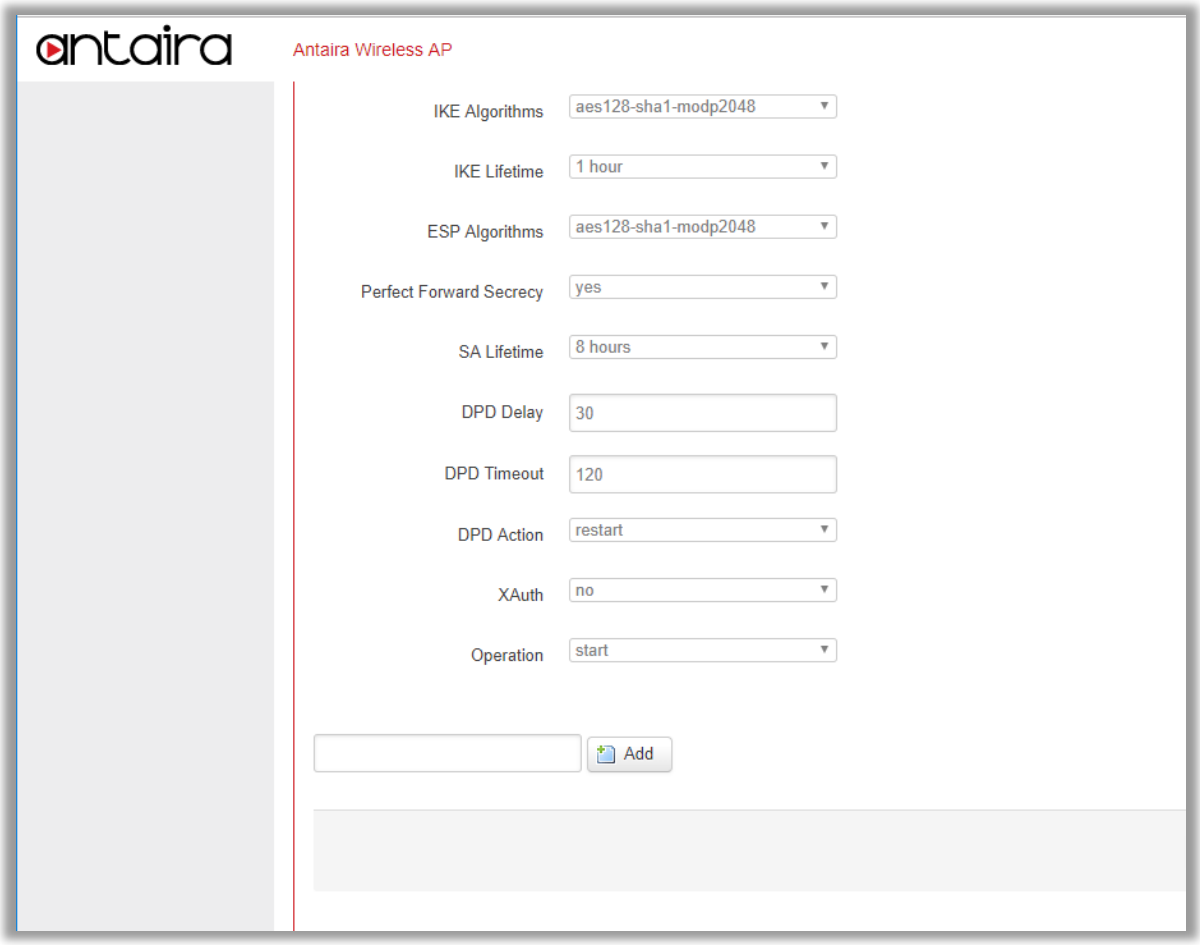
Item	Description
NAT Traversal	To enable/disable IPSec NAT Traversal function.
Add Button	Create a tunnel name and press add button to add an IPSec tunnel configuration template.



Item	Description
KEv1/IKEv2	(1) permit: no IKEv2 should be transmitted, but will be accepted if peer sites initiate with IKEv2. (2) no: only uses IKEv1, and no IKEv2 negotiation will be transmitted or accepted. (3) yes: allows IKEv1 and IKEv2, and uses IKEv2 to start the negotiation by default. (4) insist: only IKEv2 is allowed, and IKEv1 will be rejected.
Local Peer IP	The outgoing IP address of the Antaira wireless AP. It will automatically detect if default route is configured.
Local Subnet	The private subnet behind the Antaira wireless AP. Format is IP/mask length.
Local ID	The identity of the Antaira wireless AP for IKE negotiation.
Remote Peer IP	The peer side IP address for IPSec tunnel.
Remote Subnet	The private subnet behind the peer side for IPSec tunnel.
Remote ID	The identity of peer side for IKE negotiation.
Auth By	(1) secret: pre-shared key combined with 4.6.11 (2) rsasig: RSA signature combined with 4.6.12~4.6.15
PSK Key	Pre-shared key for IPSec tunnel.



Item	Description
CA	Root CA Certificate.
Local Certificate	The certificate of the Antaira wireless AP for IKE negotiation.
Local Key	The private key of the Antarira wireless AP for IKE negotiation.
Remote Certificate	The certificate of the peer side for IKE negotiation.



Item	Description
IKE Algorithms	The security parameters for IKE phrase 1 negotiation. It supports the following combination: 3des-md5-modp1024, 3des-md5-modp2048, 3des-sha1-modp1024, 3des-sha1-modp2048, aes128-md5-modp1024, aes128-md5-modp2048, aes128-sha1-modp1024, aes128-sha1-modp2048, aes256-sha1-dh22, aes256-sha1-dh23, aes256-sha1-dh24.
IKE Lifetime	The lifetime of IKE phrase 1 negotiation. Before timeout, the IKE phrase 1 will be re-negotiated.
ESP Algorithm	The security parameters for IKE phrase 2 negotiation. It supports the following combination: 3des-md5-modp1024, 3des-md5-modp2048, 3des-sha1-modp1024, 3des-sha1-modp2048, aes128-md5-modp1024, aes128-md5-modp2048, aes128-sha1-modp1024, aes128-sha1-modp2048, aes256-sha1-dh22, aes256-sha1-dh23, aes256-sha1-dh24.
Perfect Forward Secret	Perfect Forward Secret security feature for IKE negotiation.

SA Lifetime	The lifetime of IKE phrase 2 negotiation. Before timeout, the IKE phrase 2 will be re-negotiated.
DPD Delay	The delay in seconds between Dead Peer Detection keepalives (R_U_THERE, R_U_THERE_ACK).
DPD Timeout	The length of time in seconds that there are no DPD keepalives and no traffic. After this time period, DPD action will be performed.
DPD Action	(1) hold: keeps the security parameters in the Antaira Wireless AP. (2) clear: clears the security parameters in the Antaira Wireless AP. (3) restart: re-negotiates the security parameters.
XAuth	(1) no: disables XAuth authentication option. (2) yes: enables XAuth authentication option.
Username	The username for XAuth.
Password	The password for XAuth.
Operation	(1) start: the IKE will be initiated for this tunnel when the Antaira Wireless AP is booted up. (2) ignore: the IKE will not be initiated for this tunnel when the Antaira Wireless AP is booted up.