ALTAI
Super WiFi

Configuration Guide
Version 1.2

Altai A8n (ac) Series
Super WiFi Base Station

Altai Technologies Ltd. All rights reserved

Copyright © 2015 Altai Technologies Limited

ALL RIGHTS RESERVED.

Altai Technologies Limited
Unit 209, 2/F, Lakeside 2,
10 Science Park West Avenue,
Hong Kong Science Park,
Shatin, New Territories,
Hong Kong

Telephone: +852 3758 6000
Fax: +852 2607 4021
Web: www.altaitechnologies.com

Customer Support Centre:
Email: support@altaitechnologies.com

Altai Technologies Ltd. All rights reserved

Radio Frequency Interference Requirements

This device complies with Part 15 of FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.
3. This device should not be co-located or operating in conjunction with any other antenna or transmitter.

Interference Statement

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

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 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.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the

Altai Technologies Ltd. All rights reserved

party responsible for compliance could void the user's authority to operate this equipment.

Warning

The user is advised to keep apart from the base-station and antenna with at least 45cm when the base-station is in operation.

Please install a lightning arrestor to protect the base station for lightning dissipation during rainstorms. Lightning arrestors are mounted outside the structure and must be grounded by means of a ground wire to the nearest ground rod or item that is grounded.

A8n (ac) product series require professional installation. The installer shall be responsible for ensuring that the proper 5GHz antenna is employed so that the limits in FCC Part 15.247 are not exceeded. The installer is responsible for ensuring that the 5GHz radio is used exclusively for fixed, point-to-point operations.

Disclaimer

All specifications are subject to change without prior notice. Altai Technologies assumes no responsibilities for any inaccuracies in this document or for any obligation to update information in this document. This document is provided for information purposes only. Altai Technologies reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Altai Technologies Ltd. All rights reserved

Table of contents

Altai Technologies Ltd. All rights reserved

Altai Technologies Ltd. All rights reserved

Altai Technologies Ltd. All rights reserved

Altai Technologies Ltd. All rights reserved

1.Introduction

This guide covers the initial configuration of Altai A8n (ac) Series Super WiFi Base Station via Web Administration Interface (Web UI). Web Administration Interface (Web UI) is the built-in and user-friendly graphic interface on all Altai A8n (ac) Series products. It allows you to configure, monitor, and manage the devices using web browser. Mozilla Firefox, Google Chrome, and Internet Explorer 8+ are recommended.

This guide is applicable with firmware version 2.0.1.6 or above for hardware platforms with the following models:

Product Name	**A8n (ac)**	**A8-Ein (ac)**	**A8in (ac)**
Model Number	WA8011NAC-X	WA8011NAC	WA8011NAC-H

Table 1 – A8n (ac) Series products

Altai Technologies Ltd. All rights reserved

2. Getting Started

This chapter covers the procedures for logging into / out A8n (ac) Series Products Web Administration Interface (Web UI) via Ethernet, and restarting the device via Web UI.

2.1. Preparing the Administrator Computer

1. On your Windows XP or Windows 7 computer, open the Network Connections (or Change adapter settings) control panel according to how the Start menu is set up:

On **Windows XP**, click **Start** > **Control Panel** > **Network Connections**.
On **Windows 7**, click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Change adapter settings**.

2. Right-click the icon for **Local Area Connection**, and then click **Properties**.
3. When the Local Area Connection Properties dialog box appears, select **Internet Protocol (TCP/IP)** (or **Internet Protocol Version 4 (TCP/IPv4)**) from the scrolling list, and then click **Properties**. The Internet Protocol (TCP/IP) Properties dialog box appears.
4. Write down all of the currently active network settings. You will need this information later when you restore your computer to its current network configuration.
5. Configure the IP address settings with the values listed in Table 2.

IP Address	*Any address in the 192.168.1.x, except 192.168.1.222 and 192.168.1.255* *Example: 192.168.1.2*
Subnet Mask	*255.255.255.0*
Default Gateway	Blank
DNS	Blank

Table 2 - Configure administrative computer's IP address settings

6. Click **OK** to save the changes and close the TCP/IP Properties dialog box.
7. Click **OK** again to close the Local Area Connection Properties dialog box.

Altai Technologies Ltd. All rights reserved

2.2. Connect to Your Altai Access Point

1. Connect your laptop to **Data In** port on the PoE Injector provided in the Altai's package using Ethernet cable
2. Connect the Ethernet port of AP to **Data & Power Out** port on the PoE Injector provided in the Altai's package using Ethernet cable.
3. Connect the power cord to the power port on the PoE Injector. Connect the other end of the power cord to a power outlet.

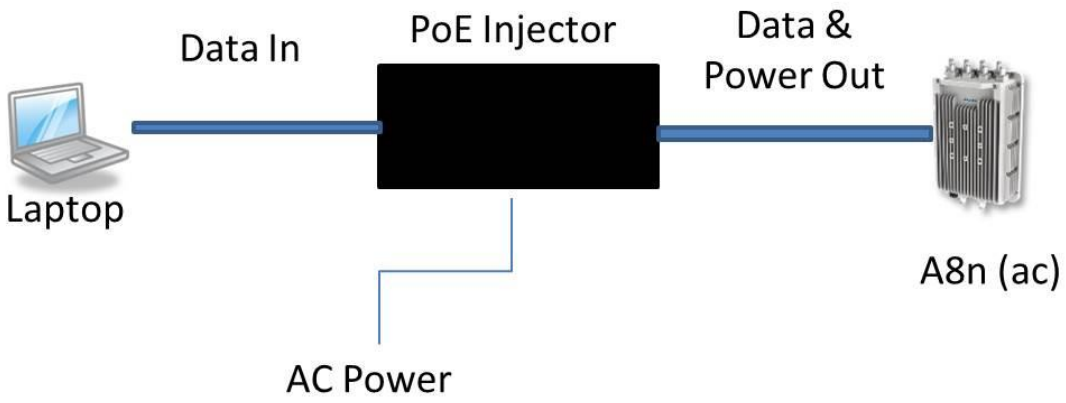


Figure 1 – A8n (ac) Connection Diagram

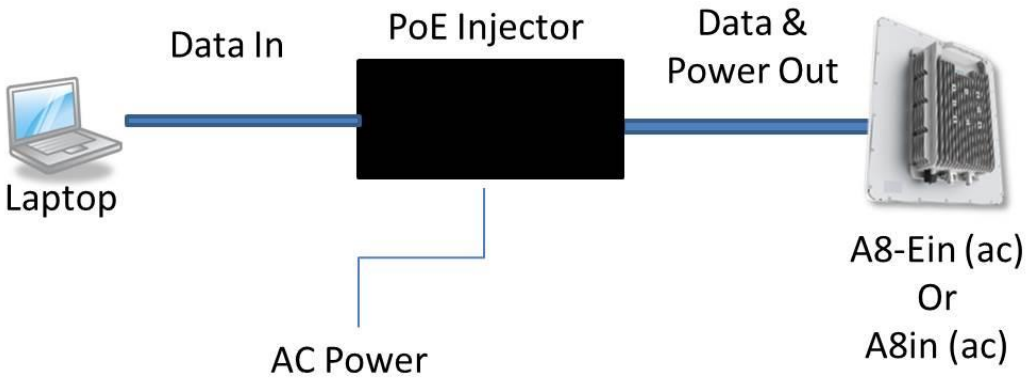


Figure 2 – A8n-Ein (ac)/ A8in (ac) Connection Diagram

4. Verify the AP's Power LED is steady green after a minute

Altai Technologies Ltd. All rights reserved

2.3. Login the AP (via Ethernet)

1. Verify the AP's Power LED is steady green
2. Open a Web browser from the computer.
3. Type http://192.168.1.222 in the address bar or location bar (see Figure 3).
4. Type *admin* (default username) in **Username**
5. Type *admin* (default password) in **Password**
6. Click **Login**

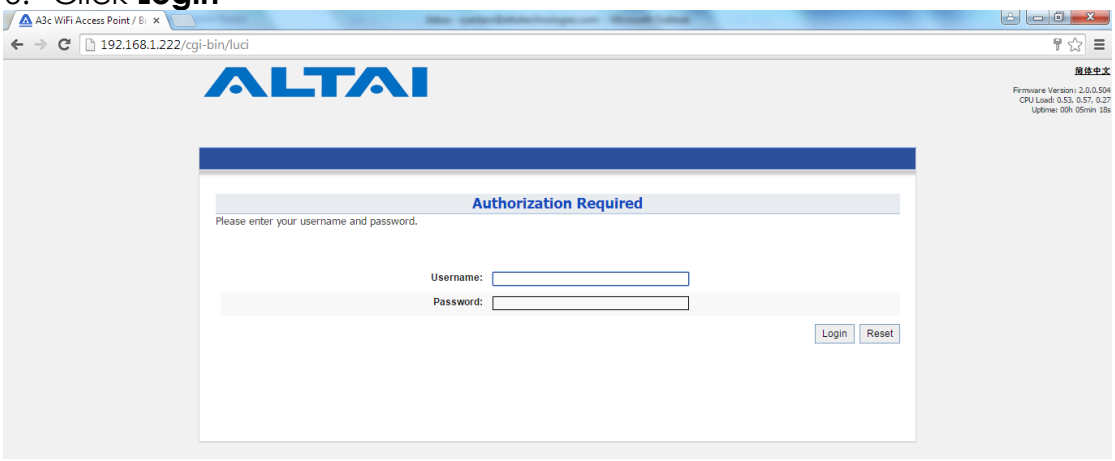


Figure 3 – A8n (ac) Series Product's Login Page

2.4. Secondary IP Address of A8n (ac) Series Products

The default IP address of A8n (ac) series products is *192.168.1.222/24*. A8n (ac) series products support a fixed IP address on the Ethernet connection called Secondary IP Address. This secondary IP address is *192.168.99.x/24* where x denotes as the decimal value of the last byte of the Ethernet MAC address on the access point.

Example 1:

Device Ethernet MAC address: 00:19:BE:20:03:**8C**

Secondary IP Address of this device:

192.168.99.**140** (**8C** (HEX) → **140** (DEC))

The secondary IP address uses IP range from *192.168.99.5/24* to *192.168.99.254/24*. The rest of IP addresses are reserved. If the last byte of a MAC address matches any of the reserved IP addresses, the supported device shall follow the MAC to IP address mapping shown in Table 3:

Altai Technologies Ltd. All rights reserved

Ethernet MAC address	Reserved Purpose	Replaced MAC byte	Secondary IP address
XX:XX:XX:XX:XX:00	Invalid IP	A0	192.168.99.160
XX:XX:XX:XX:XX:01	For gateway	A1	192.168.99.161
XX:XX:XX:XX:XX:02	For operator computer	A2	192.168.99.162
XX:XX:XX:XX:XX:03	For operator computer	A3	192.168.99.163
XX:XX:XX:XX:XX:04	For operator computer	A4	192.168.99.164
XX:XX:XX:XX:XX:FF	Invalid IP	AF	192.168.99.175

Table 3 – A8n (ac) Series Product Secondary IP Address

Example 2

Device Ethernet MAC address: 00:19:BE:20:03:**FF**

Secondary IP Address of this device:

192.168.99.**175** (**FF** (HEX) → **AF** (HEX) → **175** (DEC))

2.5. Interface Guide

Figure 4 – AP Status Overview

Web Administration Interface (Web UI) consists of five primary tabs:

Status Tab - show system status information, including system status, interfaces status, and system logs.

Altai Technologies Ltd. All rights reserved

Configuration Tab – allow the configuration of device operation parameters, including system setting, network settings, and wireless LAN settings.
Administration Tab – allow the management of device, including user administration, certification, SNMP, firmware update, factory reset, configuration backup / restore, and customization.
Tools Tab – provide tools for radio planning, diagnosis, and device's maintenance.
About Tab – show product information, including hardware version, firmware version.

Also, Web UI has a quick tools bar on its top-right hand corner in all pages. It provides some quick tools and basic information. They are chosen language, device reboot, system logs download, and configuration application …etc.

2.6. Logout from Web UI

1. Click **Logout** on top-right hand corner of Web UI

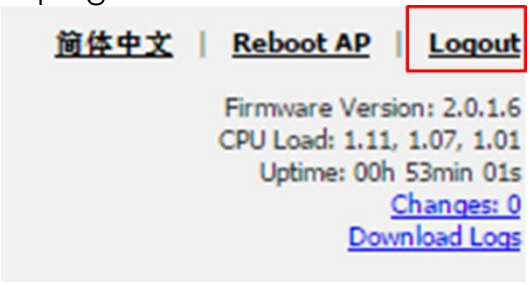


Figure 5 – Logout from Web UI

2. Click **OK**

2.7. Reboot AP via Web UI

1. Click **Reboot AP** on top-right hand corner of Web UI
2. Click **Perform reboot**

Figure 6 – Reboot the device via Web UI

Altai Technologies Ltd. All rights reserved

3.Summary of Basic Configuration Tasks

This chapter summarizes the quick setup procedures for configuring A8n (ac) Series products to operate in different roles in your network, including Access Point (AP), Station (CPE/STA), and Repeater.

3.1. Configure as Access Point (AP)

1. Go to **Configuration** > **Network** > **General > WAN Settings**
2. Select suitable internet connection type (DHCP / Static)

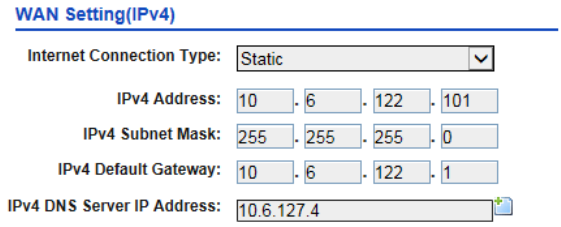


Figure 7 – WAN Setting (IPv4)

3. Configure IP Address on the device (static internet connection only)
4. Click **Submit**
5. For 2.4G Radio: Go to **Configuration** > **Wireless** > **Radio0(2.4G) > General**
   For 5G Radio: Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**

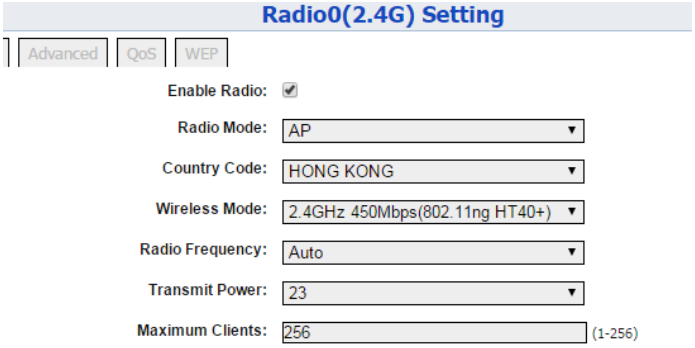


Figure 8 – 2.4G Radio General Setting of AP

6. Select *AP* in **Operating Mode**
7. Select suitable **Country Code** that matches your device's installation location.
8. Select suitable **Wireless Mode**
   802.11 ng HT20 is recommended option on 2.4G radio;
   802.11 ac HT80 is recommended option on 5G radio
9. Select the suitable **Radio Frequency**.
10. Select the suitable **Transmission Power.**
11. Click **Submit**

Altai Technologies Ltd. All rights reserved

12. For 2.4G Radio: Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN**
    For 5G Radio: Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN**

Figure 9 – Radio 2.4G WLAN List

13. Provide unique **SSID** on each enabled WLAN
14. Click **Submit**
15. For 2.4G Radio: Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
    For 5G Radio: Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**

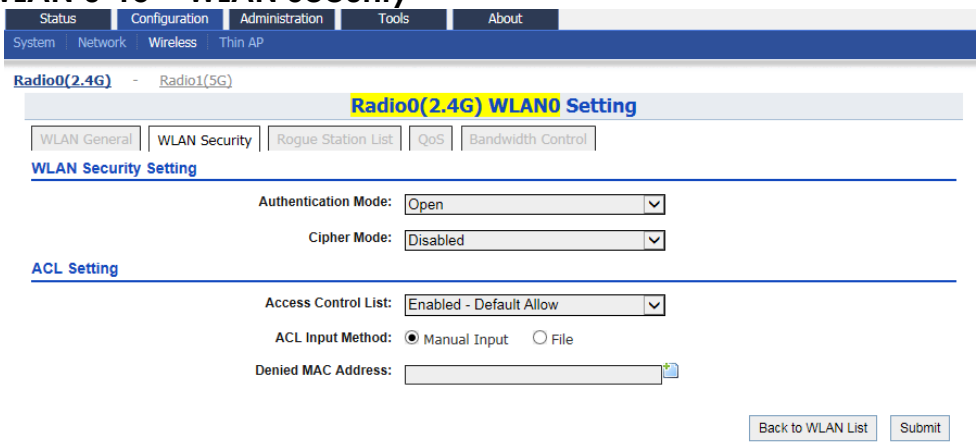


Figure 10 – Radio 2.4G WLAN0 Security Setting

16. Setup suitable settings of **WLAN Security** on each operating WLAN
17. Click **Submit**
18. Save and apply the settings

Altai Technologies Ltd. All rights reserved

3.2. Configure as Station (CPE/STA) (5G radio only)

1. Go to **Configuration** > **Network** > **General > WAN Settings**
2. Select your ISP's internet connection type (DHCP / Static)
3. Configure IP Address on the device (for static internet connection type only)
4. Click **Submit**
5. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**

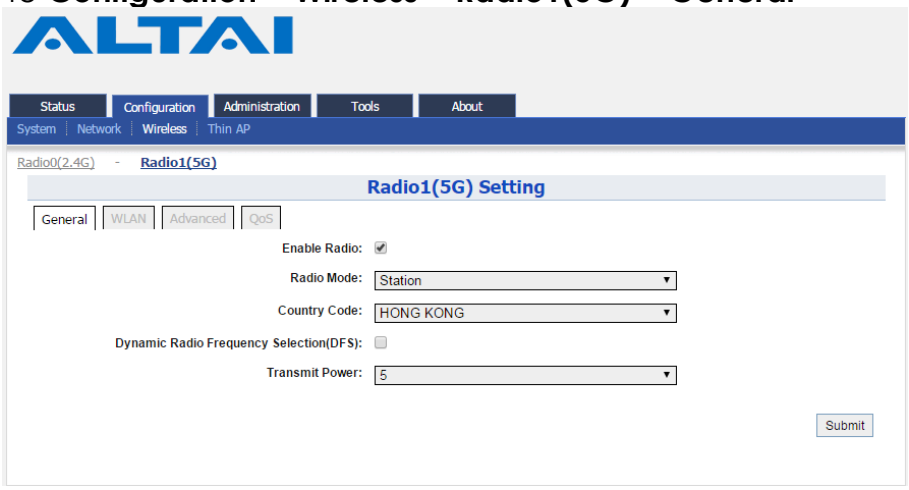


Figure 11 –5G Radio General Setting of Station

6. Select *Station* as **Operating Mode** on 5G radio the device.
7. Select suitable **Country Code** that matches your device's installation location.
8. Select the suitable **Transmission Power.**
9. Click **Submit**
10. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **More…**

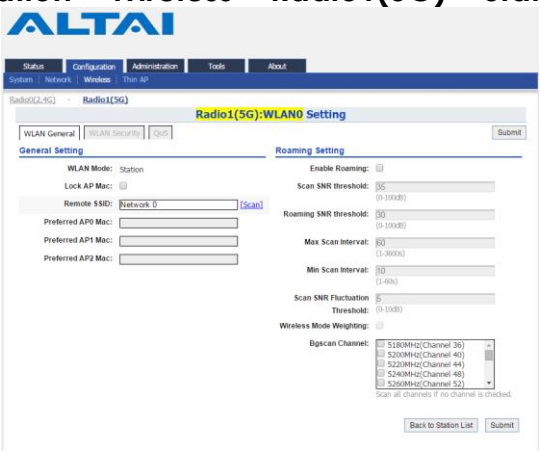


Figure 12 – 5G Radio WLAN Setting of Station

11. Scan and select the suitable SSID your ISP provides
12. Click **Submit**
13. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN Security**

Altai Technologies Ltd. All rights reserved

14. Setup suitable settings of **WLAN Security** that your ISP provides
15. Click **Submit**
16. Save and apply the settings

Altai Technologies Ltd. All rights reserved

3.3. Configure as Repeater

1. Go to **Configuration** > **Network** > **General > WAN Settings**
2. Select suitable internet connection type (DHCP / Static)
3. Configure IP Address on the device (for static internet connection type only)
4. Click **Submit**
5. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**

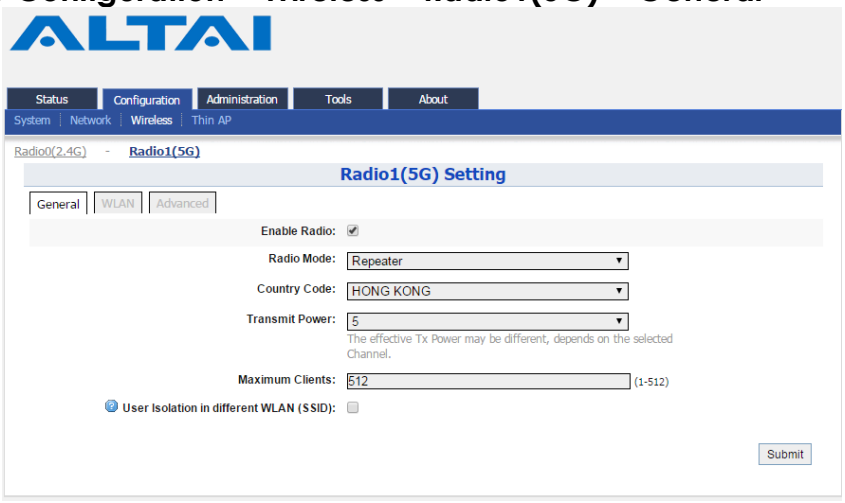


Figure 13 – 5G Radio General Setting of Repeater

6. Select *Repeater* as **Operating Mode** on 5G radio the device.
7. Select suitable **Country Code** that matches your device's installation location.
8. Select the suitable **Transmission Power**
9. Click **Submit**

Altai Technologies Ltd. All rights reserved

10. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN 0-15** > **More…**

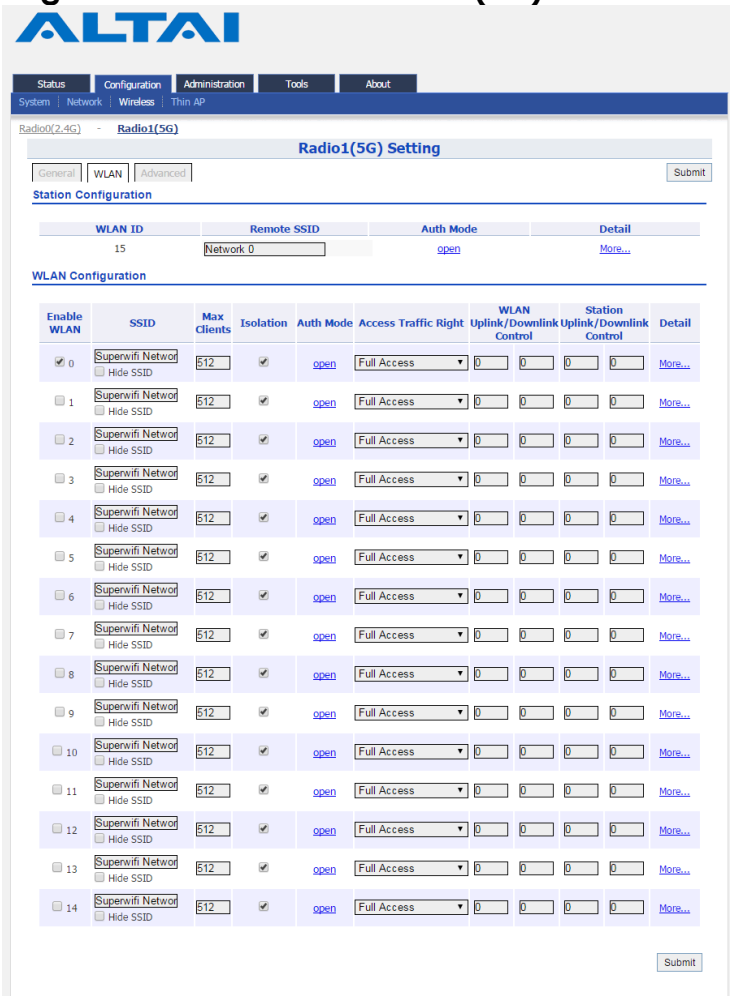


Figure 14 – 2.4G Radio WLAN List

11. Scan and select the suitable SSID from remote AP that your device associate with on WLAN 15
12. Setup suitable settings of **WLAN Security** that matches the remote AP
13. Click **Submit**
14. Provide unique **SSID** on each operating WLAN
15. Setup suitable settings of **WLAN Security** on each operating WLAN
16. Click **Submit**
17. Save and apply the settings

Altai Technologies Ltd. All rights reserved

4. Configure Your Access Point

This chapter covers the AP configurations including network configuration, wireless configuration, VLAN … etc.

Notes:

- *Click **Submit** to submit the modified configuration into temporary memory*
- *Click **Save & Apply** (top-right hand corner) to apply the modified configuration*
- *Click **Unsaved Change** (top-right hand corner) to review all modified configuration in temporary memory*

Hints:

- *You should click **Submit** to submit all changes on the same configuration page.*
- *You may click **Save & Apply** to apply all submitted change at the end of configuration*

Altai Technologies Ltd. All rights reserved

4.1. Basic Configurations

This section covers the basic configuration on A8n (ac) Series products.

4.1.1. Synchronize AP's system clock with NTP server

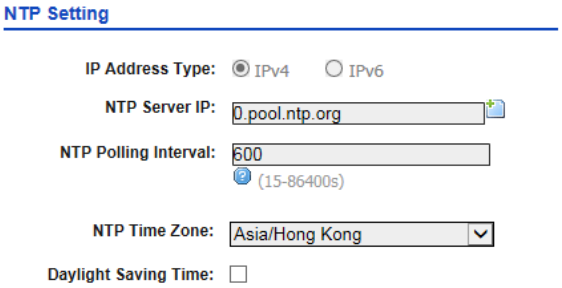


Figure 15 – NTP Setting

1. Go to **Configuration** > **System**
2. Change the following settings:
   NTP Server IP – Type in either the domain name / IP address of NTP server which you want to synchronize with.
   NTP Polling Interval – Type in the interval in second between each synchronization request from the AP to NTP server. The default setting is 600 seconds
   NTP Time Zone – Select the appropriate time zone. The default setting is *Asia/Hong Kong*
   Daylight Saving Time – Select the checkbox if your place has daylight saving time
3. Click **Submit**
4. Click **Save & Apply**

Note:

- ***IP Address Type*** *is changed by AP automatically based on whether* ***IPv6*** *is enabled or not*
- *If providing NTP server's domain name in* ***NTP Server IP****, you must provide valid DNS server information (see 4.1.2 on page 15 for more detail). Otherwise, NTP setting cannot take effect.*

Altai Technologies Ltd. All rights reserved

4.1.2. Assign Internet Connection Type for AP (IPv4) – Static / DCHP

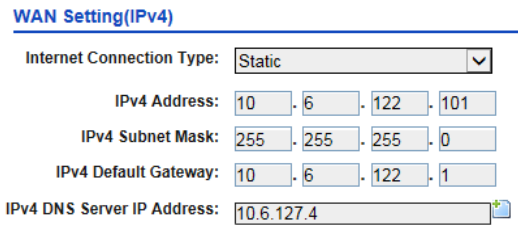


Figure 16 – WAN Settings (IPv4)

1. Go to **Configuration** > **Network** > **General > WAN Settings**
2. Change the following settings:
   Internet Connection Type – configure AP either as a client with fixed IP address or DCHP client;

Static	Stand for Static IP addressing; AP will not update its IP address automatically
DHCP Client	Require an IP address from DCHP server on the network; AP renews its IP address periodically

   IPv4 Address –Type in an IP address for AP (Static Internet Connection Type only)
   IPv4 Subnet Mask – Type in a subnet mask for AP (Static Internet Connection Type only)
   IPv4 Default Gateway – Type in an IP address of default gateway for AP (Static Internet Connection Type only)
   IPv4 DNS Server – Type in IP address of one or more DNS server for AP (Static Internet Connection Type only).

   Note:
   - Click for adding more DNS;
   - Click to remove existing DNS server entry

3. Click **Submit**
4. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.1.3. Configure Radio Interface as Access Point (AP)

Radio 0 – 2.4GHz Radio

Radio General Configuration

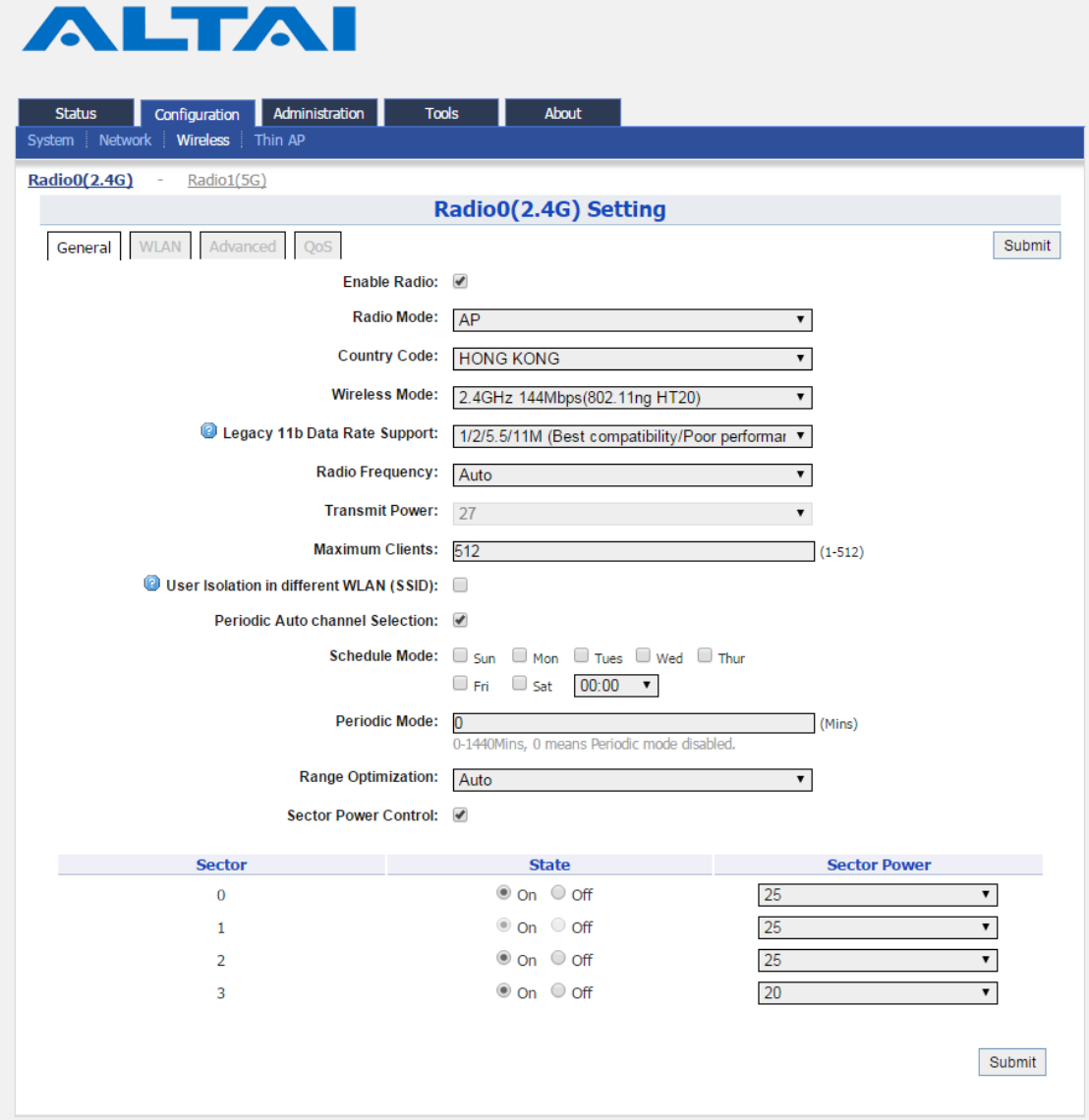


Figure 17 – Radio0 (2.4G) General Settings of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G) > General;**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *AP in* **Radio Mode**
4. Change the following settings:
   Country Code – Select an option that matches your device's installation location; *Hong Kong* is the default setting.

Altai Technologies Ltd. All rights reserved

Note:

- Country code enforces regulatory restrictions on radio frequencies and maximum transmission power that the AP can operate in.

Wireless Mode – Select suitable Wi-Fi operating mode for the AP;
2.4G 11Mbps (802.11 b)
2.4G 54Mbps (802.11 bg)
2.4G 54Mbps (802.11 g-only)
2.4G 144Mbps (802.11 ng HT20); Default Setting
2.4G 144Mbps (802.11 n-only HT20)
2.4G 300Mbps (802.11 ng HT40+)
2.4G 300Mbps (802.11 n-only HT40+)
2.4G 300Mbps (802.11 ng HT40-)
2.4G 300Mbps (802.11 n-only HT40-)

Legacy 11b Data Rate Support [Optional] – Select a suitable option for the legacy client compatibility. In order to enhance the spectrum efficiency, low data rates (1/2/5.5/11M) should be eliminated. The options include:

1/2/5.5/11M (Best compatibility /Poor performance)	All legacy clients will be supported
5.5/11M (Good compatibility /Good performance)	Clients only capable of 1/2Mbps will not be supported
Disable All (Poor compatibility/ Best performance)	Clients only capable of 802.11b standard will not be supported

Note:

- 2.4G 11Mbps (802.11 b) is not applicable.

Radio Frequency – Choose the operating channel for the radio interface; AP selects the channel with the least amount of interference if *Auto* is selected. An optional feature **Periodic Auto channel Selection** will be shown if *Auto* is selected. *2412MHz (Channel 1)* is the default setting

Note:

- Select the radio frequency based on the result of channel scan is recommended

Transmission Power – Select the total transmission power for the radio interface.
Maximum Client – Specify the maximum associated client between *1* and *512* that the radio interface serves. 512 is the default setting.

Altai Technologies Ltd. All rights reserved

Disable HT20/HT40 Auto Switch [Optional] – If select the checkbox, AP will NOT switch the channel width between 20 MHz and 40 MHz automatically. This option is only available if *any wireless mode with HT40+/-* is selected.

User Isolation in different WLAN (SSID) [Optional] - Select the checkbox to block the users' communication across different SSID in the AP directly.

Periodic Auto Channel Section [Optional] – Select the checkbox to enable a scheduled channel selection task on the radio interface.

Schedule Mode Select exact time and day(s) for selecting radio frequency for the interface

Periodic Mode Select a countdown timer (minute) for selecting radio frequency for the interface; *0* denotes disable.

Range Optimization [Optional] – Select a coverage range for optimization. 'Auto' is the default value.

Sector Power Control [Optional] – Select the checkbox to enable a feature to assign a transmitting power for each sector.

5. Click **Submit**
6. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

WLAN List

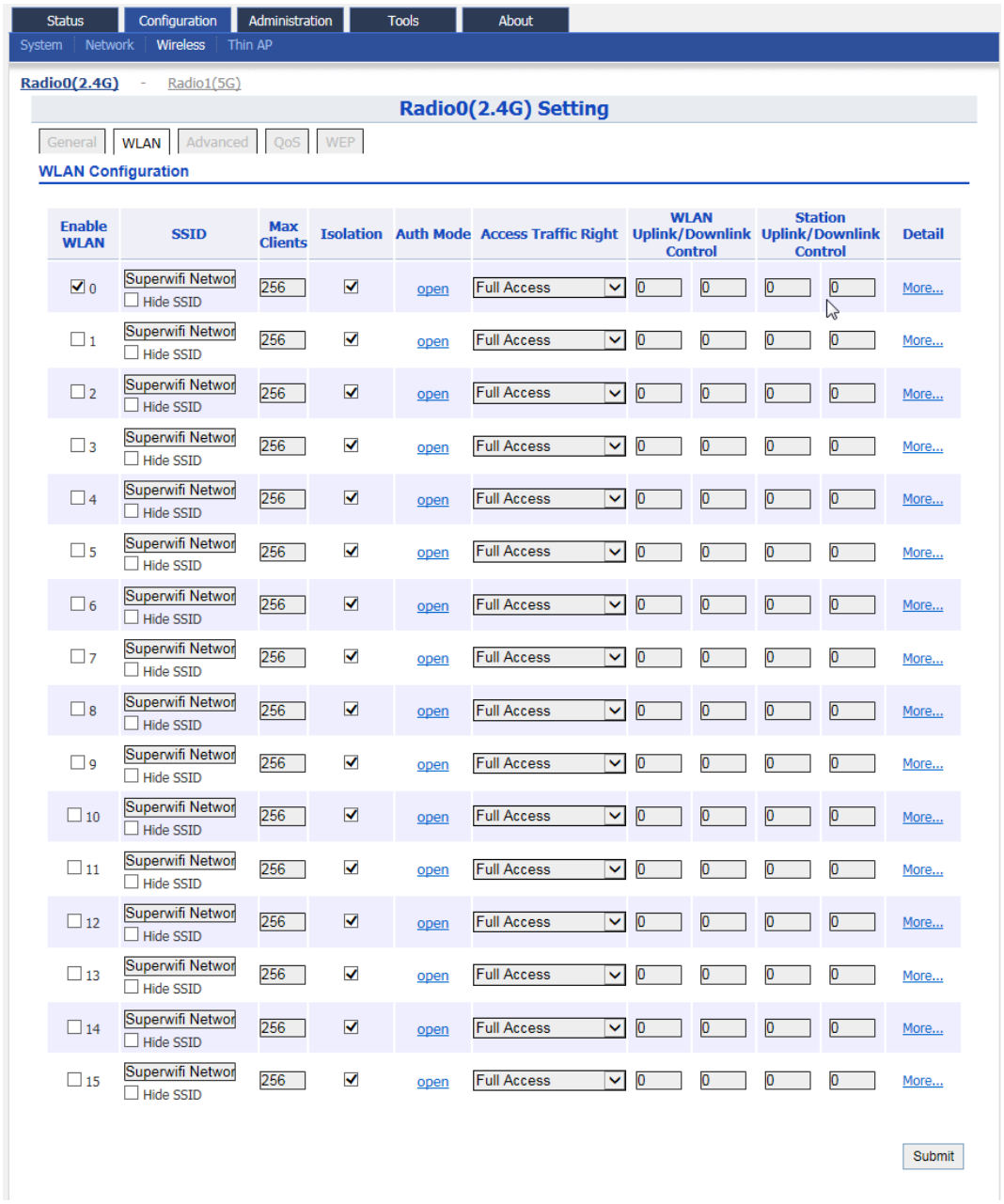


Figure 18 – WLAN List of Radio0(2.4G) of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN**
2. Select **Enable WLAN** checkbox to enable the WLAN 0 – 15 individually;

Note:
- A8n (ac) products support up to 16 WLANs on its Radio0

3. Click **Submit**
4. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

WLAN 0-15 General Configuration

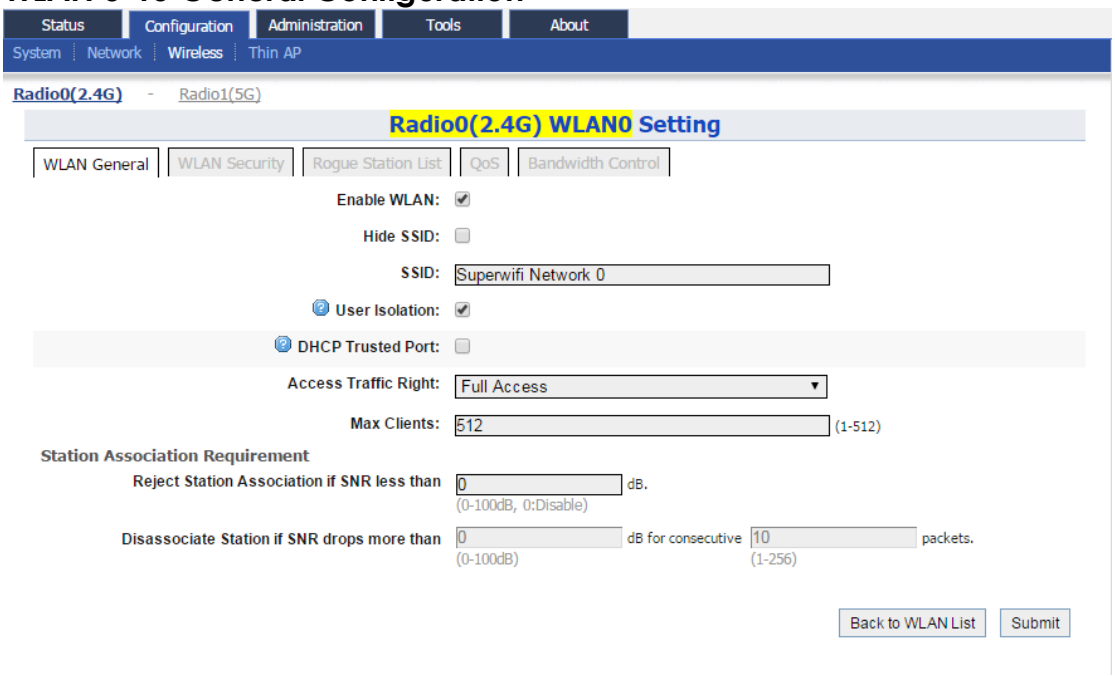


Figure 19 – WLAN Detail Settings of WLAN 0 of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN 0-15** > More…
2. Change the following settings:
   Hide SSID [Optional] – Select the checkbox to hide SSID name from its beacon frame
   SSID – Provide a unique name for the particular WLAN

Note:
- If you want to configure the same SSID on two different WLAN; their security setting MUST be different from each other.

User Isolation [Optional] – Select the checkbox to block user communication within the same SSID in the AP directly.
DHCP Trust Port [Optional] - Deselect the checkbox to prevent illegal DHCP servers offering IP address to DHCP clients via this WLAN.
Access Traffic Right – Specify the privilege of associated clients;

Full Access	Associated client can access Internet and manage AP
AP Management Only	Associated client can manage AP only, but not able to access the Internet
AP Management Disable	Associated client can access the Internet, but not able to manage AP

Max Clients - Specify the maximum associated clients between *1* and *512* on this WLAN. *512* is the default setting.

Note:
- **Max Clients** in WLAN 0 – 15 MUST be smaller than or equal to (≥) the **Max Clients** setting in 0 Radio General Configuration

Altai Technologies Ltd. All rights reserved

Station Association Requirement [Optional] – Specify and additional requirement on Signal Strength to Noise Ratio (SNR) for associated clients.

Reject Station Association if SNR less than X dB	denote the minimum SNR level which allow clients to associate; You can select any integer between *0*dB and *100*dB; *0* denotes as disable; *0* is default setting
Disassociate Station if SNR drops more than Y dB for consecutive Z packets	Y denotes the SNR tolerance; Z denotes the number of consecutive packets their SNR are below the difference of X - Y.

Notes:

- Example for Station Association Requirement with the following settings:
  Reject Station Association if SNR less than *30* dB (X = 30);
  Disassociate Station if SNR drops more than *20* dB for consecutive *10* packets (Y = 20; Z = 10)
  Consequence:
  AP accepts the clients to associate if the SNR of packets from the clients is high than (>) 30dB;
  AP kicks out the associated client if the SNR of 10 consecutive packets is below (<) 10 dB (30 dB – 20 dB)

3. Click **Submit**
4. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

WLAN 0-15 Security Configuration

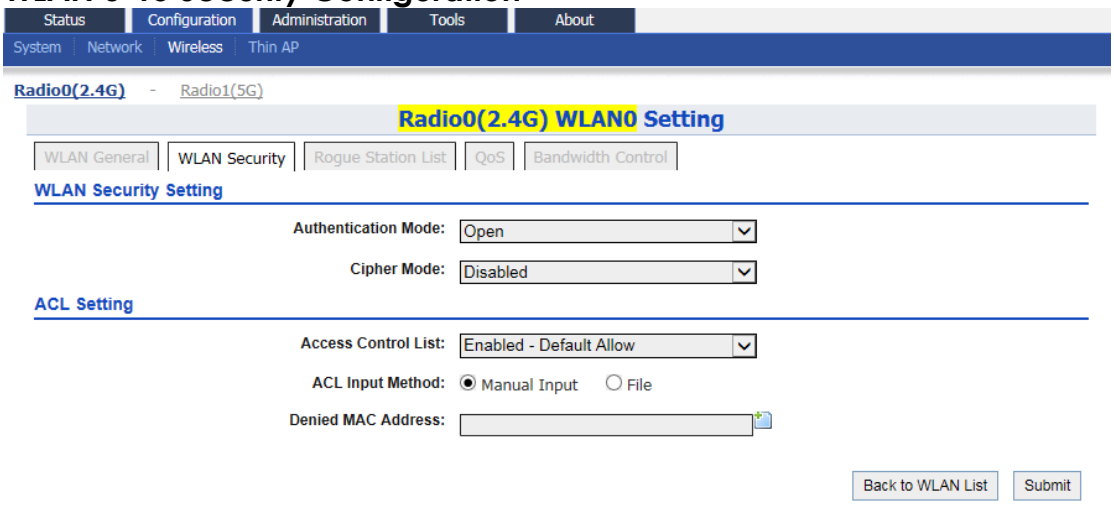


Figure 20 – WLAN Security Setting for WLAN 0 of AP

Configure WLAN as Open network

This option is typically only used in a guest network. No security measure is enforced.

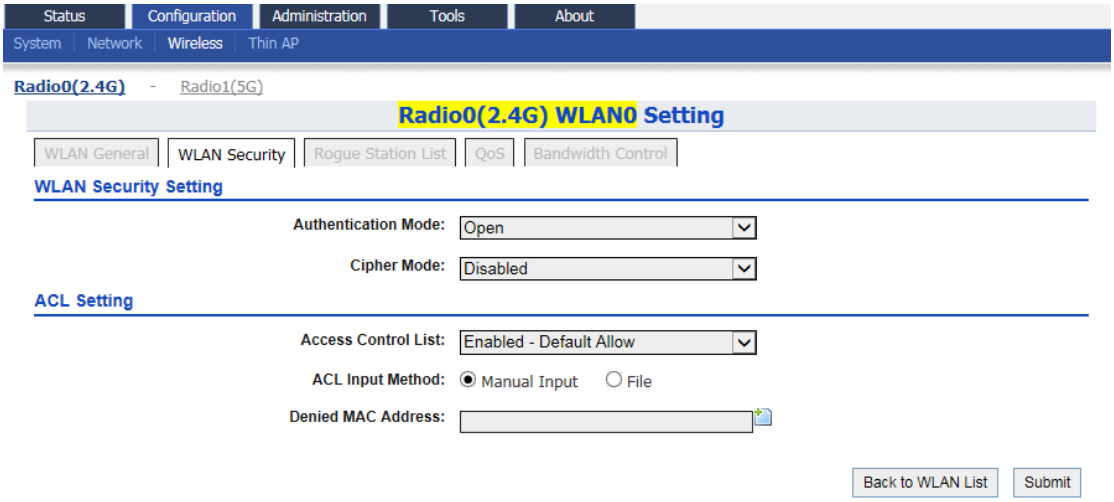


Figure 21 – Open network of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select Open in **Authentication Mode**
3. Select *Disabled* in **Cipher Mode**
4. Click **Submit**
5. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Configure WLAN as Open network with WEP encryption

This option provides minimal security as it allows all requesting devices to join a given network.

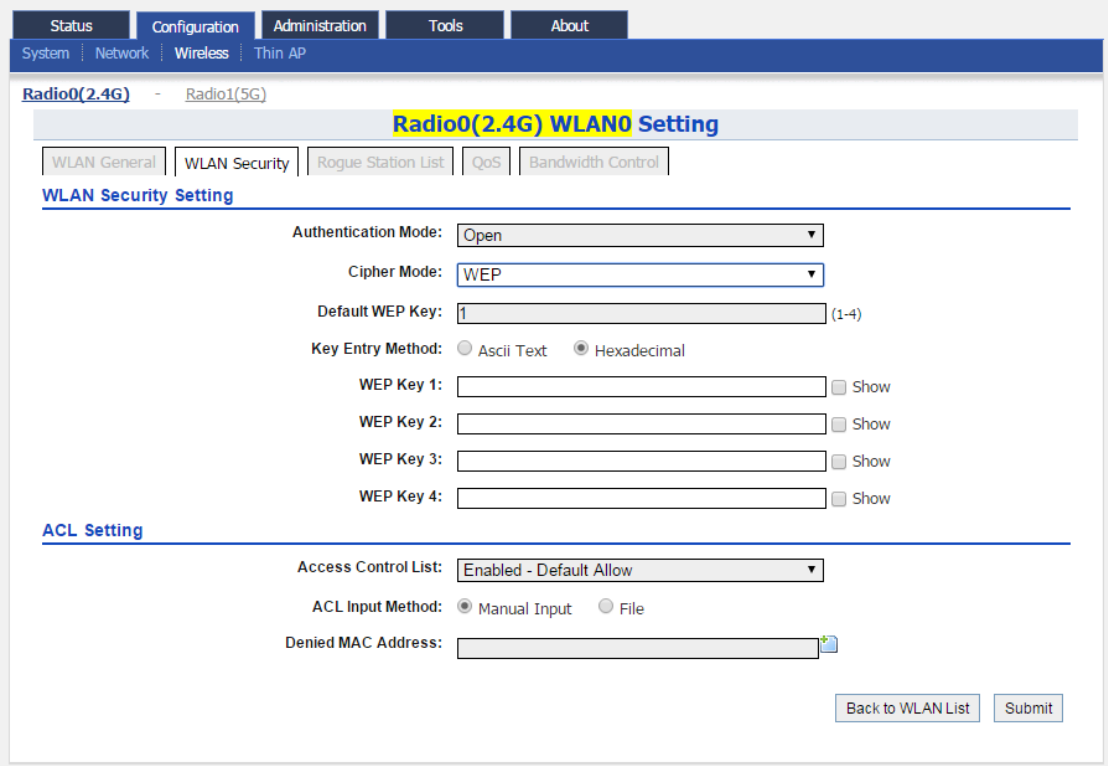


Figure 22 – Open network with WEP encryption of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *WEP* in **Cipher Mode**
4. Select key number *1 – 4* in **Default WEP Key**
5. Select **Key Entry Method**
   Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z)
   Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)
6. Type in up to four keys in **WEP Key 1**, **WEP Key 2**, **WEP Key 3** and **WEP Key 4** respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
7. Click **Submit**
8. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Configure WLAN with Shared Key Authentication

Shared Key authentication is one of the authentication methods with WEP encryption. It verifies that station has knowledge of a shared secret.

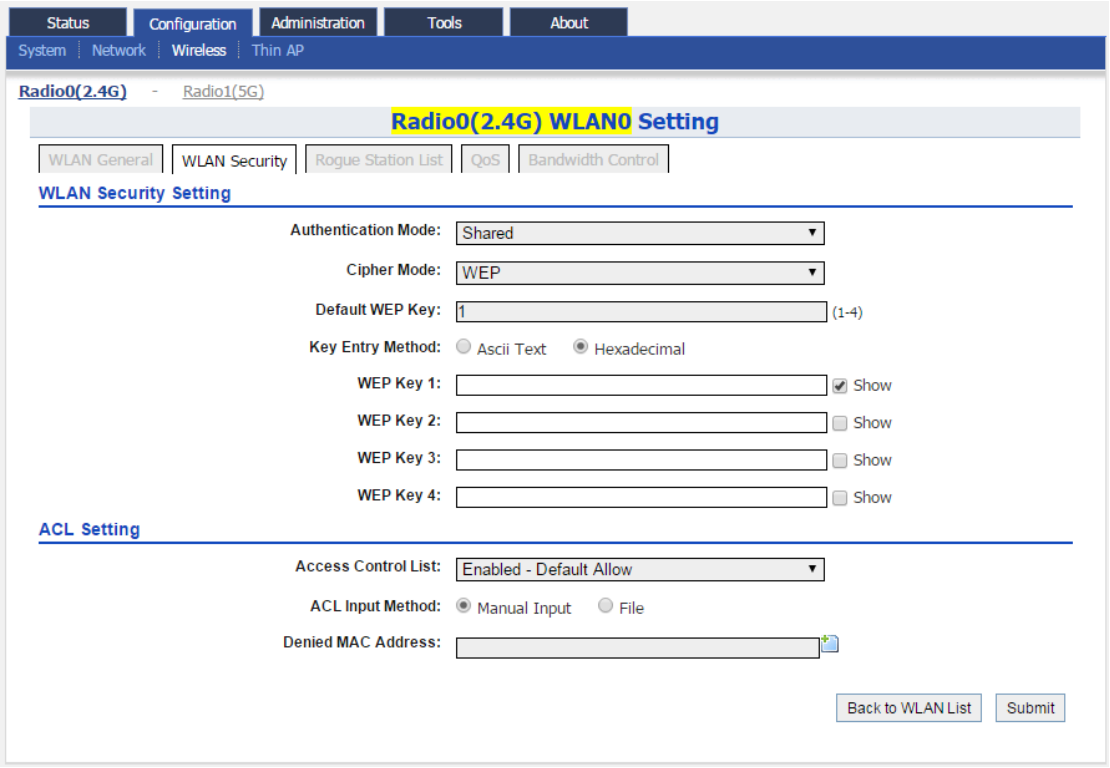


Figure 23 – Shared Key Authentication of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select *Shared* in **Authentication Mode**
3. Select *WEP* in **Cipher Mode**
4. Select key number *1 – 4* in **Default WEP Key**
5. Select **Key Entry Method**
   Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z)
   Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)
6. Type in up to four keys in **WEP Key 1**, **WEP Key 2**, **WEP Key 3** and **WEP Key 4** respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
7. Click **Submit**
8. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Configure WLAN with WPA / WPA2 / WPA-auto Authentication

WPA (Wi-Fi Protected Access) or WPA2 provides enhanced security over WEP, and allows client authentication based on an external authentication server such as a RADIUS server, for corporate networks. WPA-auto is a mixed security mode which supports multiple implementations of the WPA standard, such as WPA and WPA2.

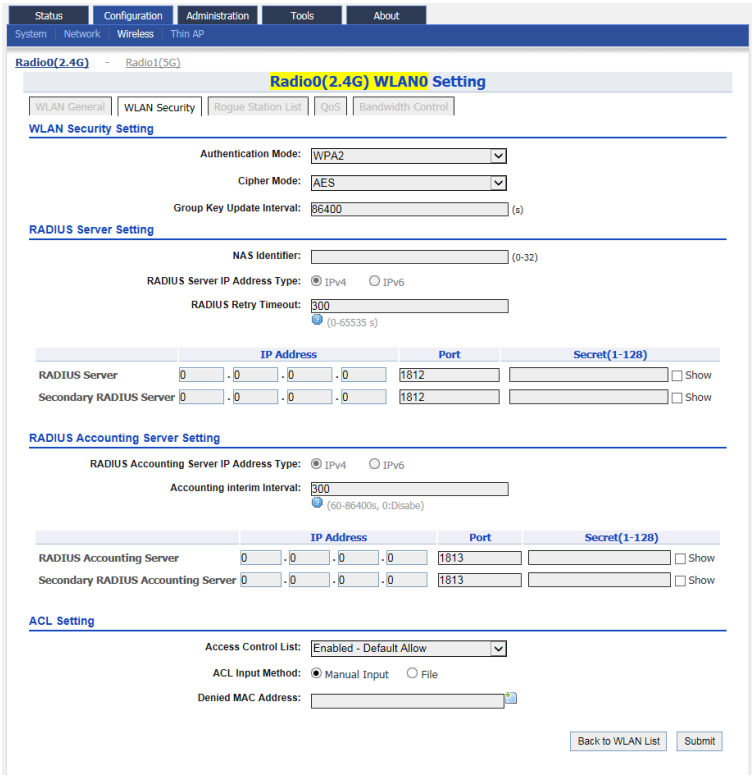


Figure 24 –WPA2 setting of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select *WPA / WPA2 / WPA-auto* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:
   If Authentication Mode is *WPA:*
   TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities
   TKIP - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
   AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

   If Authentication Mode is *WPA2*:
   AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

Altai Technologies Ltd. All rights reserved

If Authentication Mode is *WPA-auto*:
TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:
- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

4. Provide suitable identification in **NAS identifier**. Remote RADIUS server use this ID to identify its clients [WPA or WPA2 only]
5. Provide transmission timeout interval between *0* and *86400*s in **RADIUS Retry Timeout** [Optional]. *300* is default setting.
6. Provide IP address of remote RADIUS server for authentication in **IP Address of RADIUS Server**
7. Provide service port of remote RADIUS server in **Port of RADIUS Server**. *1812* is default setting.
8. Provide suitable secrets in **Secret of RADIUS Server**. It is used along with the MD5 hashing algorithm to obfuscate passwords. This secret MUST be as the same as that in RADIUS server.
9. Repeat step 7-9 if the backup RADIUS server is available.
10. RADIUS Accounting Server Setting is *optional*; you may select if the WLAN requires accounting service from remote RADIUS server. You can change the following settings:
    Accounting interim Interval - indicates the number of seconds between each interim update in seconds; *300* is default setting.
    IP Address - IP address of remote RADIUS Accounting Server
    Port - Service port of remote RADIUS server for accounting service. *1813* is default setting.
    Secret - Password MUST be as the same as that in RADIUS server

11. Click **Submit**
12. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication

Use of WPA or WPA2 provides enhanced security over WEP, and allows client authentication based on either a pre-shared key (PSK), for home or small office networks. WPA-auto-PSK is a mixed security mode which supports multiple implementations of the WPA standard, such as WPA-PSK and WPA2-PSK.

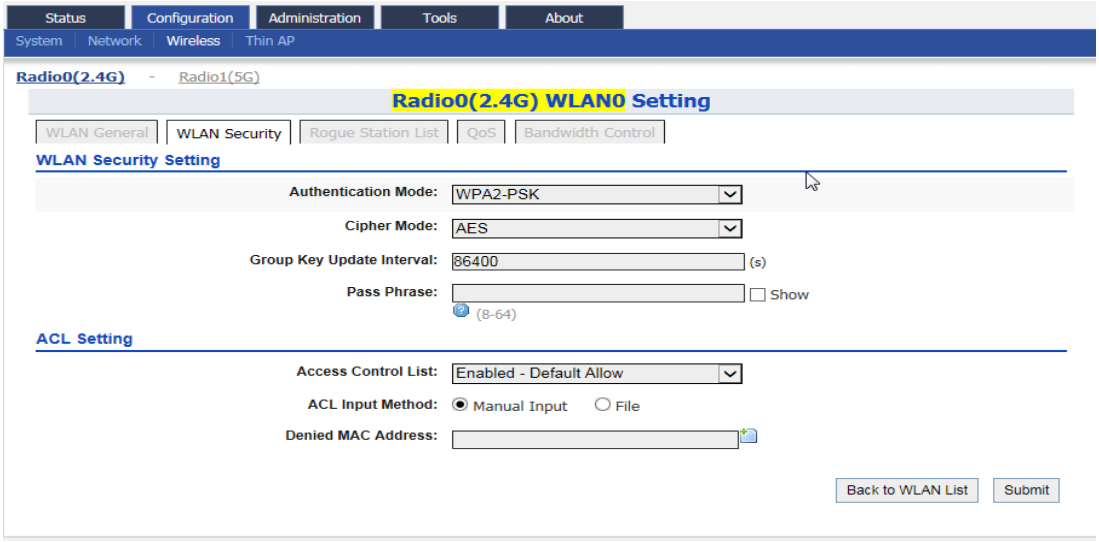


Figure 25 – WPA2-PSK Setting of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select *WPA-PSK / WPA2-PSK / WPA-auto-PSK* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:

   If Authentication Mode is WPA-PSK:

   TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities

   TKIP - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.

   AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

   If Authentication Mode is WPA2-PSK:

   AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

   If Authentication Mode is WPA-auto-PSK:

   TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities

Note:

- TKIP is not supported by 802.11n standard. If selected TKIP, the 802.11n's devices will be limited to 802.11g transfer rate, i.e. up to 54 Mbps

Altai Technologies Ltd. All rights reserved

4. Provide time in second in **Group Key Update Interval** [Optional]. *86400* is default setting.
5. Type in a string between 8 and 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
6. Click **Submit**
7. Click **Save & Apply**

Configure WLAN with WAPI Authentication

WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese National Standard for Wireless LANs (GB 15629.11-2003).

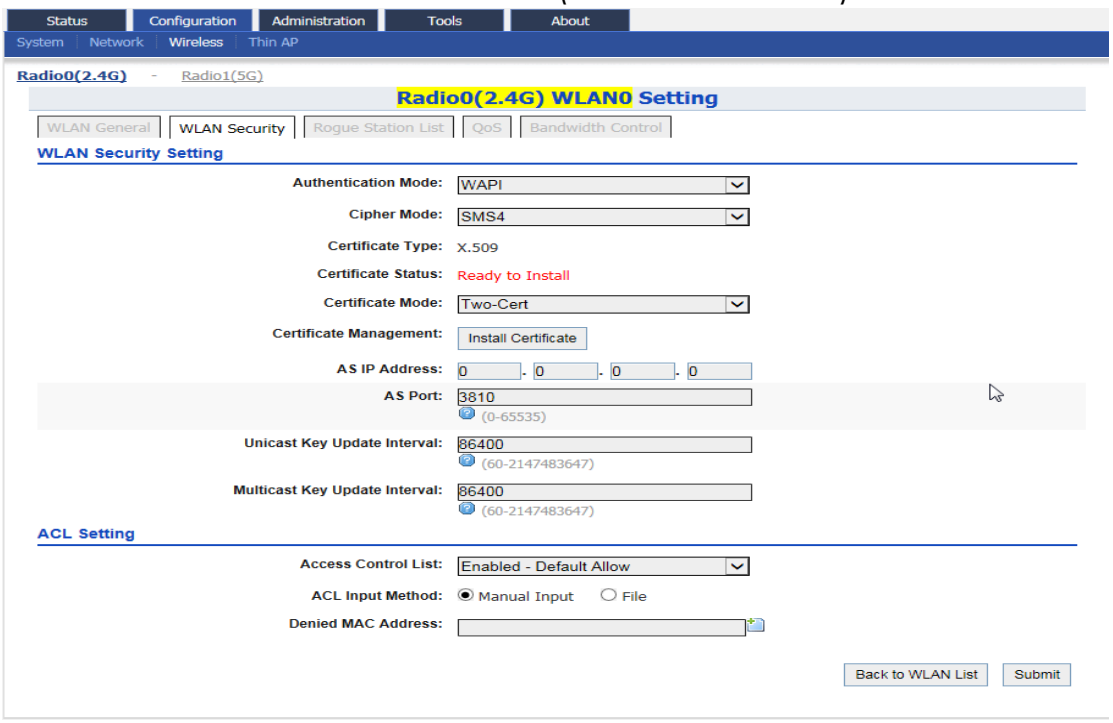


Figure 26 – WAPI Settings of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select *WAPI* in **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Select suitable option in **Certificate Mode**:
   Two-Cert – Wi-Fi client is verified by the certification from authentication server (AS) and Access Point (AP)
   Three-Cert - Wi-Fi client is verified by the certification from authentication server (AS), access point (AP), and certificate authority (CA)
5. Click **Install Certificate**; a window for installing certificate is shown (see Figure 27 and Figure 28)

Altai Technologies Ltd. All rights reserved

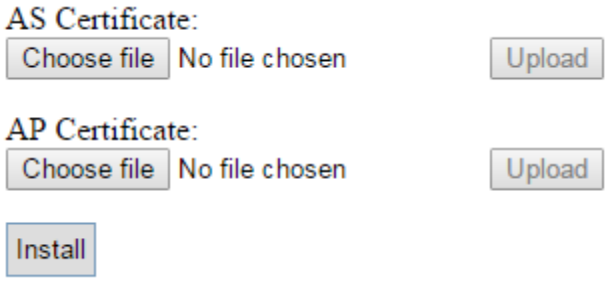


Figure 27 – Two-Cert Mode Certification Installation

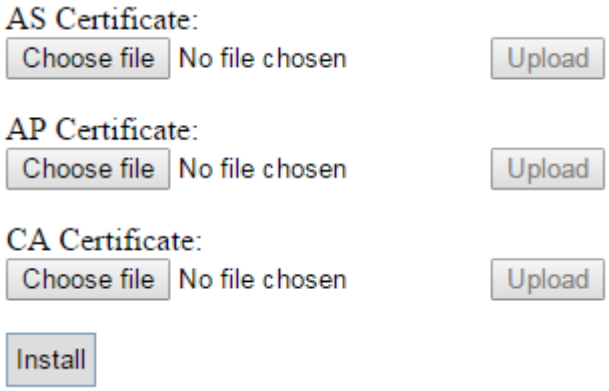


Figure 28 - Three-Cert Mode Certification Installation

6. Click **Browse** to select suitable certifications
7. Click **Upload** to upload the selected certifications to A8n (ac)
8. Click **Install** to install certifications
9. Type IP address of AS server in **AS IP Address**
10. Type service port of AS server in **AS Port**
11. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval** [Optional]; *86400* is default setting
12. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval** [Optional]; *86400* is default setting
13. Click **Submit**
14. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Configure WLAN with WAPI-PSK Authentication

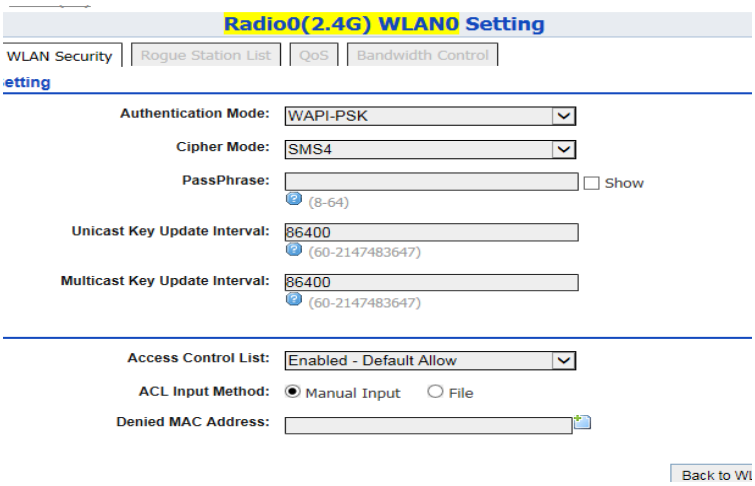


Figure 29 – WAPI-PSK Setting of AP

1. Go to **Configuration** > **Wireless** > **Radio0(2.4G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Select *WAPI* in **Authentication Mode**
3. Select *SMS4* in **Cipher Mode**
4. Type in a string between 8 and 64 characters long in **Pass Phrase** that users will use to connect to the wireless network.
5. Enter interval time between 60 and 2147483647s in **Unicast Key Update Interval** [Optional]; *86400* is default setting
6. Enter interval time between 60 and 2147483647s in **Multicast Key Update Interval** [Optional]; *86400* is default setting
7. Click **Submit**
8. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Radio 1 – 5GHz Radio

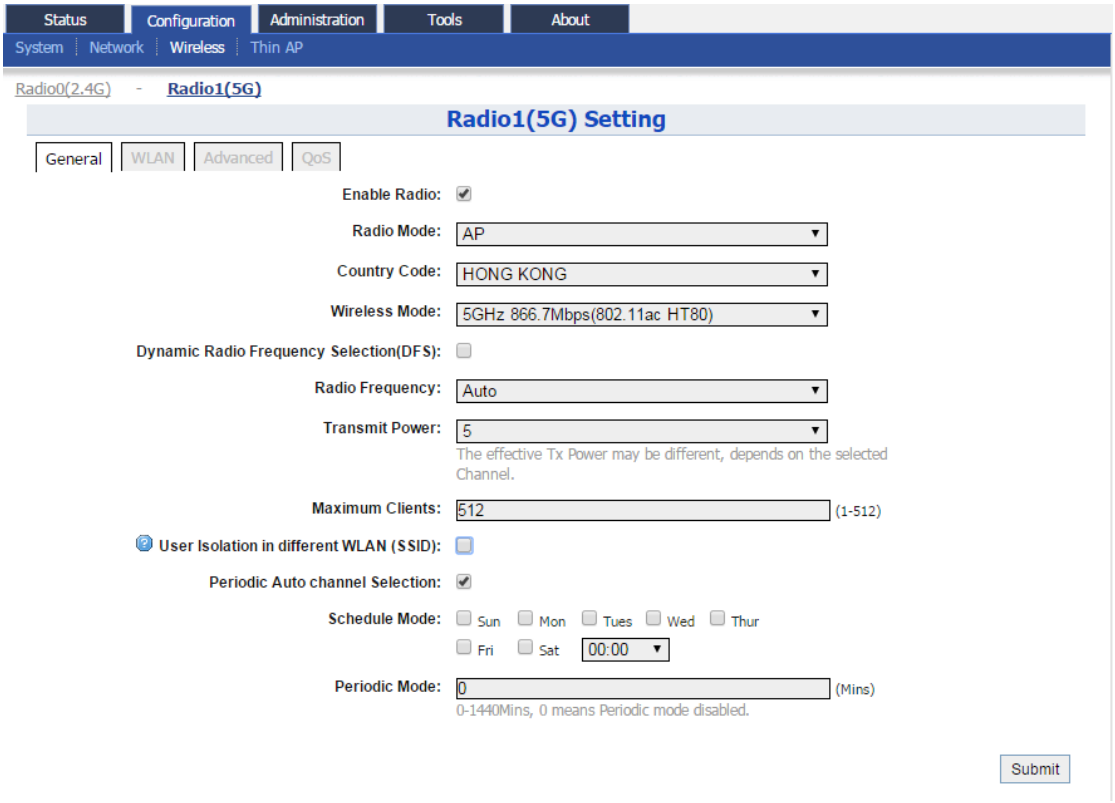


Figure 30 – Radio1 (5G) General Setting of AP

Radio General Configuration

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *AP* in **Radio Mode**
4. You can change the following settings:
   Country Code – Select an option that matches your device's installation location; *Hong Kong* is the default setting.

Note:

- Country code sets the regulatory domain for the radio frequencies and maximum transmission power that AP can use

Wireless Mode – Select suitable Wi-Fi operating mode for the AP:
5G 54Mbps (802.11 a)
5G 144Mbps (802.11 na HT20); Default Setting
5G 144Mbps (802.11 n-only HT20)
5G 300Mbps (802.11 n-only HT40+)
5G 300Mbps (802.11 na HT40+)
5G 300Mbps (802.11 na HT40-)
5G 300Mbps (802.11 n-only HT40-)
5G 173Mbps (802.11 ac HT20)
5G 400Mbps (802.11 ac HT40+)

Altai Technologies Ltd. All rights reserved

5G 400Mbps (802.11 ac HT40-)
5G 866.7Mbps (802.11 ac HT80)

Dynamic Radio Frequency Selection (DFS) – Select to enable automatic channel selection that selects the least congested channel where radar is not detected during booting up.

Note:
- **Radio Frequency** is set as *auto* if DFS is enabled

Radio Frequency – Choose the operating channel for the radio interface; AP selects the channel with the least amount of interference if *Auto* is selected. *5180MHz (Channel 36)* is the default setting
Transmission Power – Select the total transmission power for the radio interface.
Maximum Client [Optional] – Specify the maximum associated client between *1* and *512* that the radio interface serves. 512 is the default setting.
Disable HT20/HT40 Auto Switch [Optional] – If select the checkbox, AP will NOT switch the channel width between 20 MHz and 40 MHz automatically. This option is only available if *any wireless mode with 802.11n-only/na HT40+/-* is selected.
User Isolation in different WLAN (SSID): [Optional] - Select the checkbox to block the users' communication across different SSID in the AP directly.
Periodic Auto channel Section [Optional] – Select the checkbox to enable scheduled channel selection task on the radio interface:

Schedule Mode	Select exact time and day(s) for selecting radio frequency for the interface
Periodic Mode	Select a countdown timer (minute) for selecting radio frequency for the interface; *0* denotes disable.

5. Click **Submit**
6. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

WLAN List

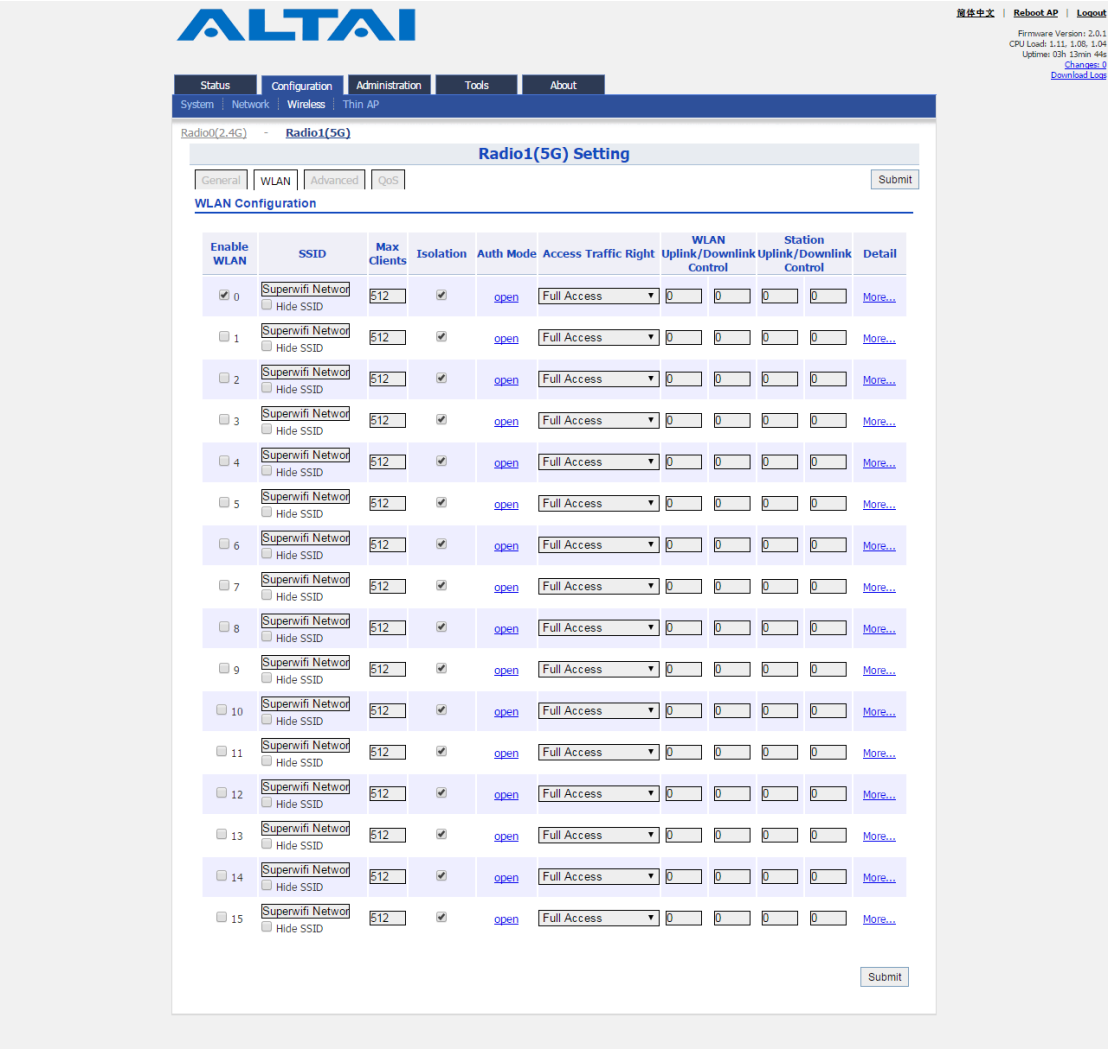


Figure 31 – WLAN list on Radio1(5G) of AP

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN**
2. Please refer to WLAN List on page 19 for more detail.

WLAN 0 - 15 General Configuration

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN 0-15** > More...
2. Please refer to WLAN 0-15 General Configuration on page 20 for more detail.

WLAN 0 - 15 Security Configuration

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN 0-15** > **WLAN Security**
2. Please refer to the following chapters for more detail:
   Configure WLAN as Open network (see Configure WLAN as Open network on page 22)
   Configure WLAN as Open network with WEP encryption (see Configure WLAN as Open network with WEP encryption on page 23)

Altai Technologies Ltd. All rights reserved

Configure WLAN with Shared Key Authentication (see Configure WLAN with Shared Key Authentication on page 24)
Configure WLAN with WPA / WPA2 / WPA-auto Authentication (see Configure WLAN with WPA / WPA2 / WPA-auto Authentication on page 25)
Configure WLAN as with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication (see Configure WLAN with WPA-PSK / WPA2-PSK / WPA-auto-PSK Authentication on page 27)
Configure WLAN with WAPI Authentication (see Configure WLAN with WAPI Authentication on page 28)
Configure WLAN with WAPI-PSK Authentication (see Configure WLAN with WAPI-PSK Authentication on page 30)

4.1.4. Configure Radio Interface as Station (STA/CPE)

Radio 0 – 2.4GHz Radio

Station radio mode is not available in Radio 0(2.4G) interface.

Radio 1 – 5GHz Radio

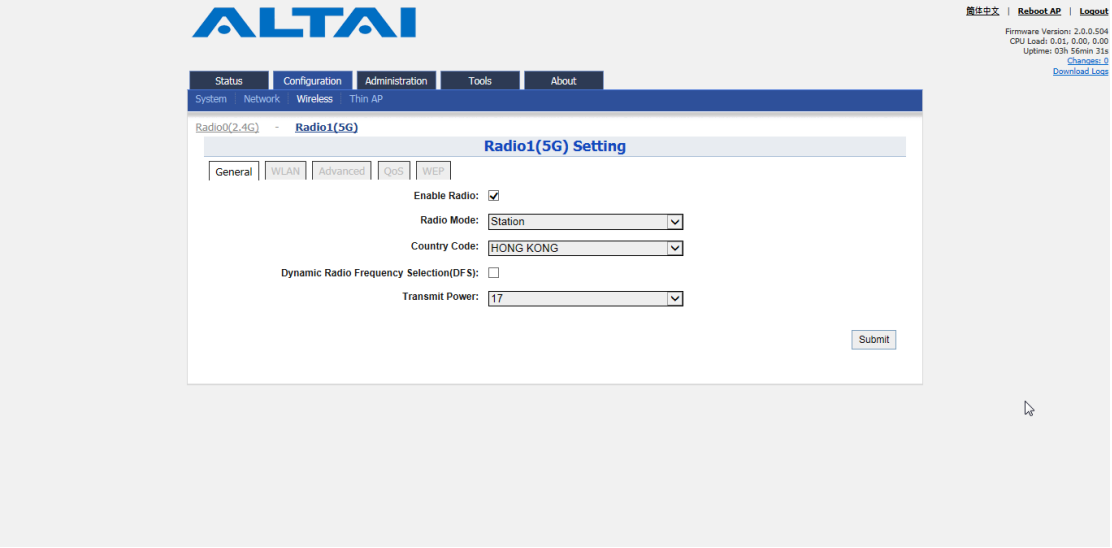


Figure 32 – Radio 1 General Setting of Station

Radio General Configuration

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **General**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *Station* in **Radio Mode**
4. Change the following settings:

Altai Technologies Ltd. All rights reserved

Dynamic Radio Frequency Selection (DFS) – Select to enable automatic channel selection that selects the least congested channel where radar is not detected during booting up.

Note:

- **Radio Frequency** is set as *auto* if DFS is enabled

Transmission Power – Select the total transmission power for the radio interface.

5. Click **Submit**
6. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Station Configuration

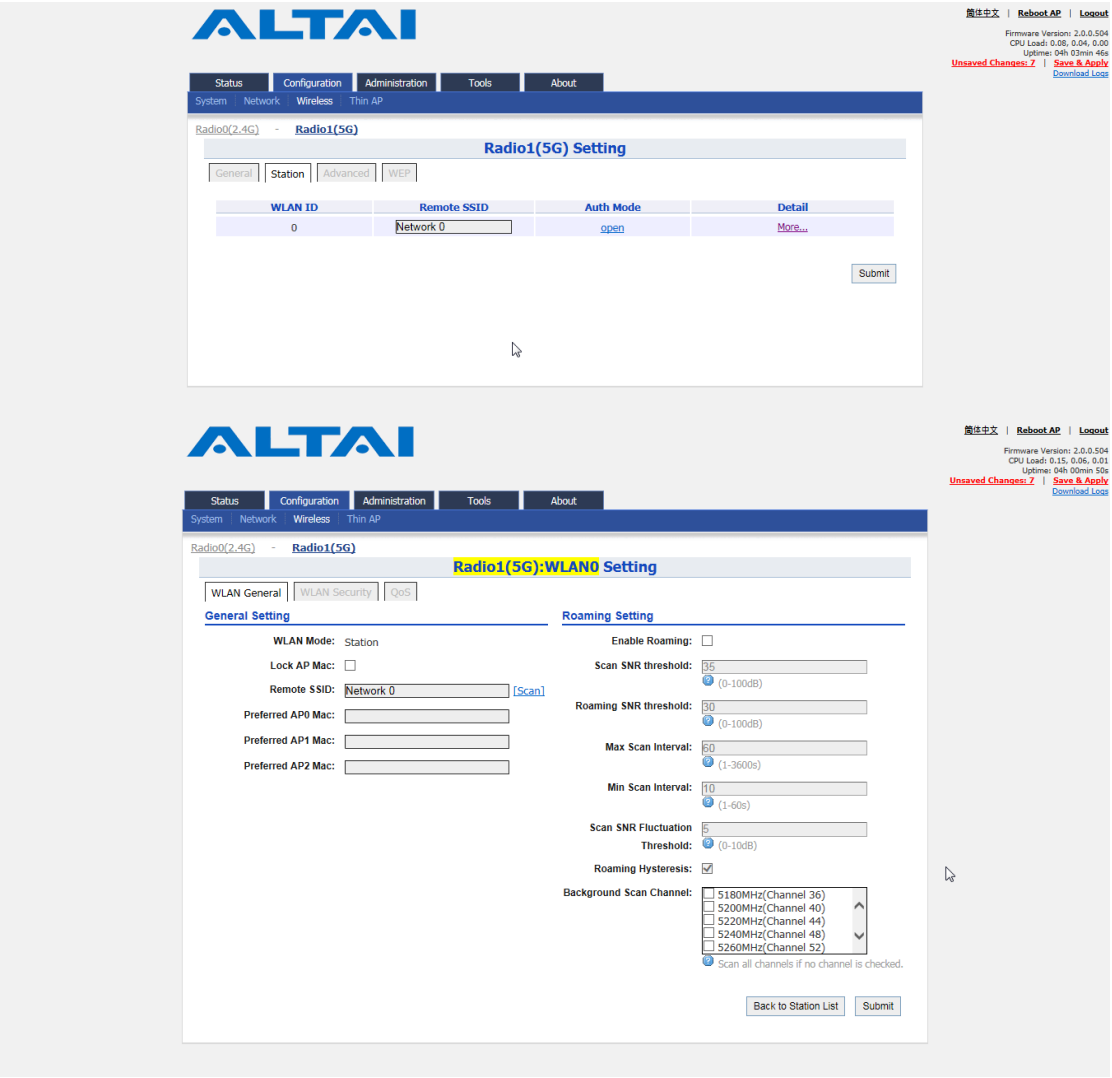


Figure 33 - Station Setting

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **More…**
2. Change the following settings:
   Lock AP Mac [Optional] – Select to force station that associate the AP with MAC address in **Remote AP MAC** only
   Remote SSID – Enter the SSID that station is going to associate. You may use **[Scan]** to look for the surrounding SSID.

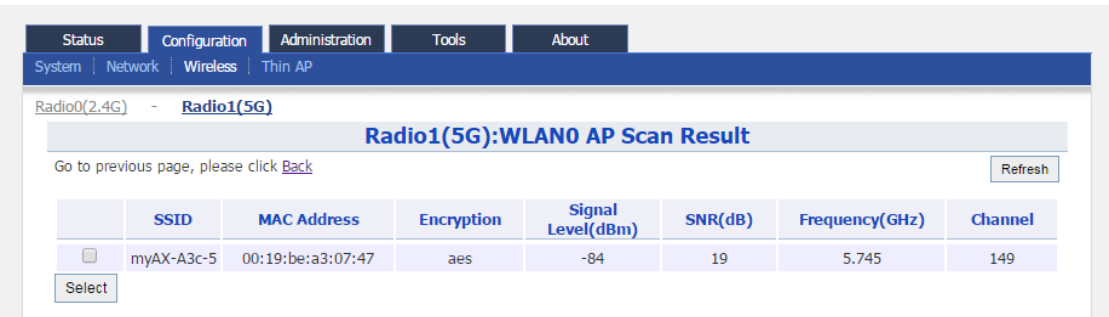


Figure 34 – SSID scan result - Station

Altai Technologies Ltd. All rights reserved

Preferred AP0 / AP1 / AP2 Mac [Optional] – Enter up to three AP MAC addresses that station associates them preferentially. AP0 is the highest priority.
Roaming Setting [Optional]
Enable Roaming - Select to enable roaming on station
Scan SNR Threshold – Enter SNR from *0*dB to *100*dB that station performs channel scanning if the SNR of received signal from associated AP is less than (<) this threshold; *35* is default setting.
Roaming SNR Threshold - Enter SNR from *0*dB to *100*dB that station triggers the roaming if the SNR of received signal from associated AP is less than (<) this threshold; *30* is default setting.

Note:
- **Scan SNR Threshold** MUST be larger than (>)**Roaming SNR Threshold**

Max Scan Interval - Specify the maximum duration from *1*s to *3600*s for channel scanning; *60*s is default setting.
Min Scan Interval - Specify the minimum duration from *1*s to *60*s for channel scanning; *10*s is default setting
Scan SNR Fluctuation Threshold – Enter SNR from *0*dB to *10*dB; the current AP's signal fluctuation (compared with previous scan result) is higher than (>) this threshold, the station will do scanning. *5*dB is default setting.
Roaming Hysteresis – Select to enable that station will be stickier to current associated AP.
Scan Channel List – Select the particular channel for scan

3. Click **Submit**
4. Click **Save & Apply**

Station Security Configuration

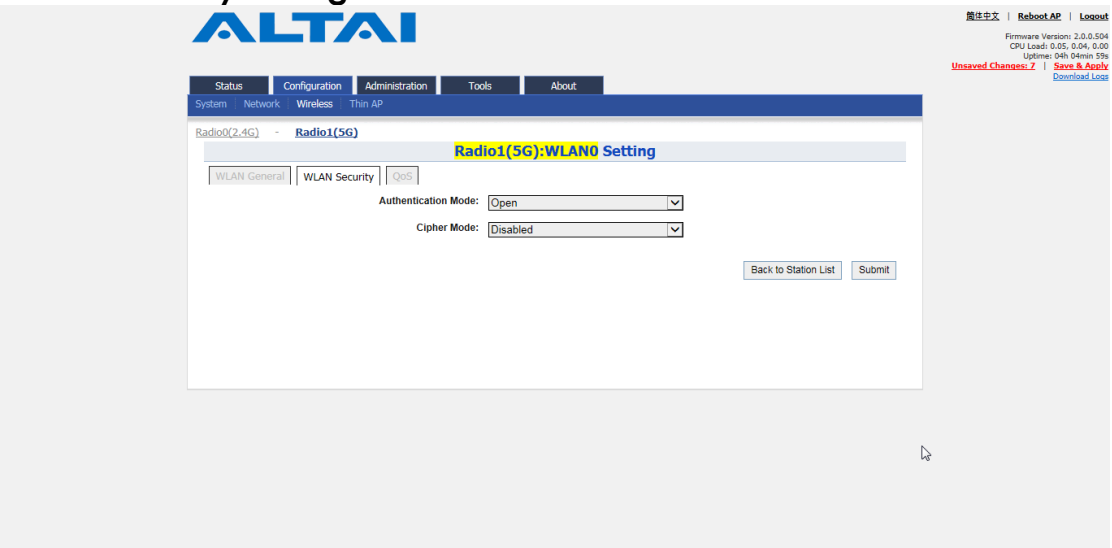


Figure 35 – Security Settings of Station

Altai Technologies Ltd. All rights reserved

Configure Station to associate Open network

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *Disabled* in **Cipher Mode**
4. Click **Submit**
5. Click **Save & Apply**

Configure Station to associate Open network with WEP encryption

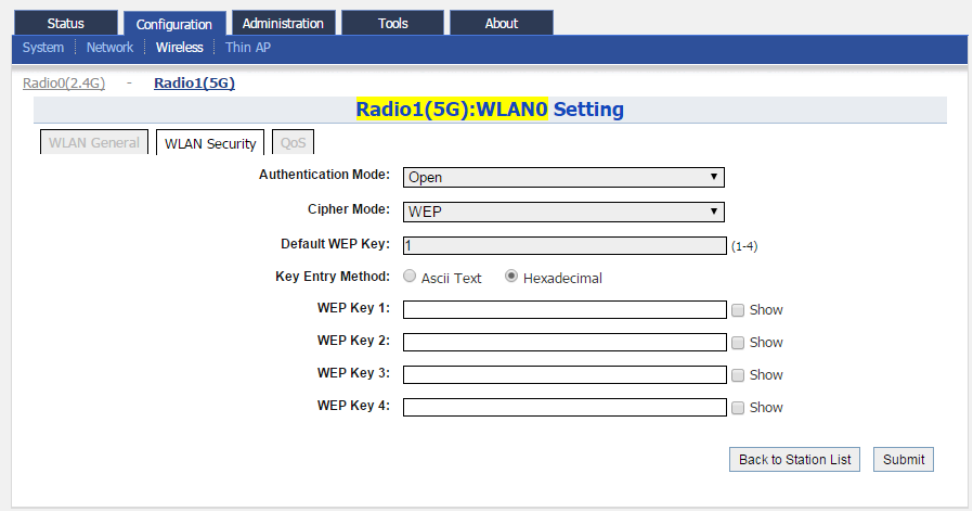


Figure 36 – Open network with WEP of Station

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN Security**
2. Select *Open* in **Authentication Mode**
3. Select *WEP* in **Cipher Mode**
4. Select key number *1 – 4* in **Default WEP Key**
5. Select **Key Entry Method**
   Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z)
   Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)
6. Type in up to four keys in **WEP Key 1**, **WEP Key 2**, **WEP Key 3** and **WEP Key 4** respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
7. Click **Submit**
8. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Configure Station to associate network with Shared Key authentication

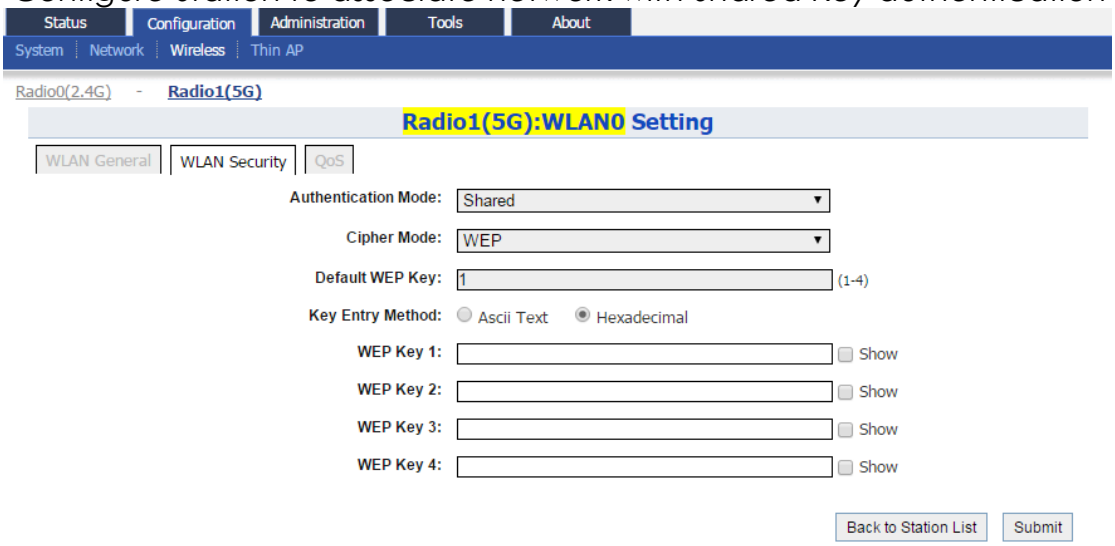


Figure 37 - Shared Key Authentication of Station

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN Security**
2. Select *Shared* in **Authentication Mode**
3. Select *WEP* in **Cipher Mode**
4. Select key number *1 – 4* in **Default WEP Key**
5. Select **Key Entry Method**
   Ascii Text key is encoded as ASCII characters (0–9, a–z, A–Z)
   Hexadecimal key is encoded as Hexadecimal characters (0–9, A–F)
6. Type in up to four keys in **WEP Key 1**, **WEP Key 2**, **WEP Key 3** and **WEP Key 4** respectively. You can type either up to 5 Ascii characters or up to 10 Hexadecimal characters as WEP Key
7. Click **Submit**
8. Click **Save & Apply**

Configure Station to associate network with WPA / WPA2 authentication

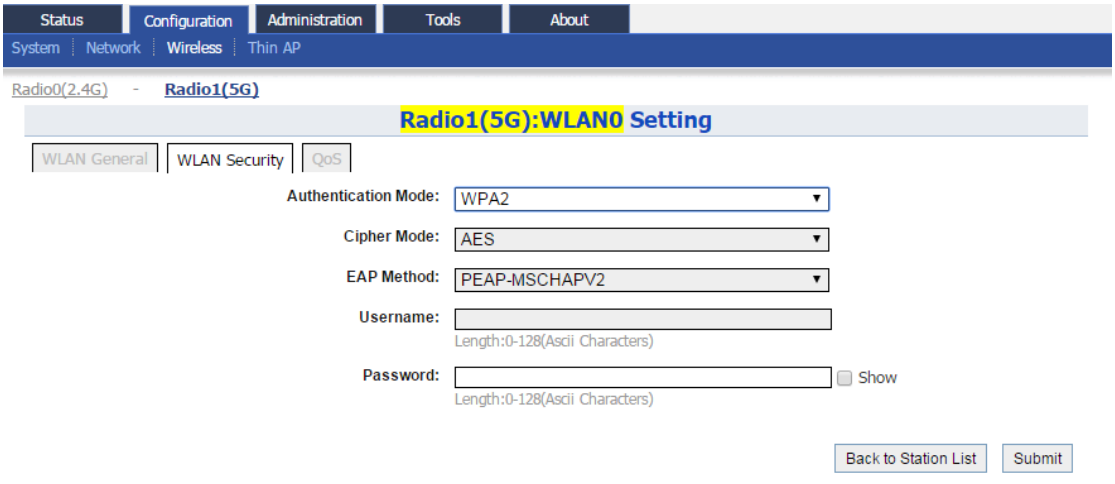


Figure 38 – WPA2 Authentication of Station

Altai Technologies Ltd. All rights reserved

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN Security**
2. Select *WPA / WPA2* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:
   If Authentication Mode is *WPA*:
   TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities
   TKIP - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
   AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.
   If Authentication Mode is *WPA2*:
   AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

4. Select suitable EAP method mode in **EAP Method**:
   PEAP-MSCHAPV2
   TTLS-MSCHAPV2
   TTPS-PAP
   TTLS-CHAP

5. Provide username in **Username** for authentication.
6. Provide password in **Password** for authentication.
7. Click **Submit**
8. Click **Save & Apply**

Configure Station to associate network with WPA-PSK / WPA2-PSK authentication

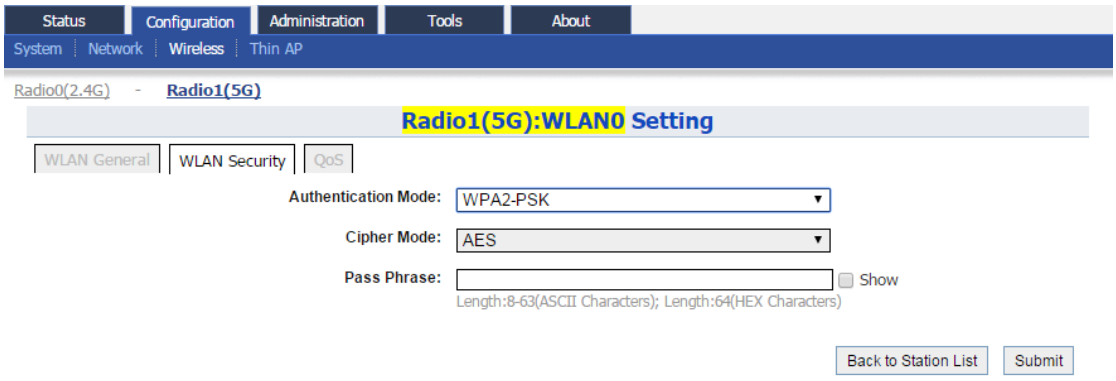


Figure 39 – WPA2-PSK Authentication of Station

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **Station** > **WLAN Security**
2. Select *WPA-PSK / WPA2-PSK* in **Authentication Mode**
3. Select suitable encryption mode in **Cipher Mode** as the followings:
   If Authentication Mode is *WPA*:
   TKIP + AES - This algorithm automatically selects TKIP or AES based on the client's capabilities

Altai Technologies Ltd. All rights reserved

TKIP - This algorithm provides greater compatibility with older client devices, but is not supported by the 802.11n standard.
AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

If Authentication Mode is *WPA2*:
AES - This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.

4. Type a string between 8 and 64 characters long in **Pass Phrase** that matches with remote AP
5. Click **Submit**
6. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.1.5. Configure Radio Interface as Repeater

Radio 0 – 2.4GHz Radio

Repeater radio mode is not available in Radio 0(2.4G) interface.

Radio 1 – 5GHz Radio

Radio General Configuration

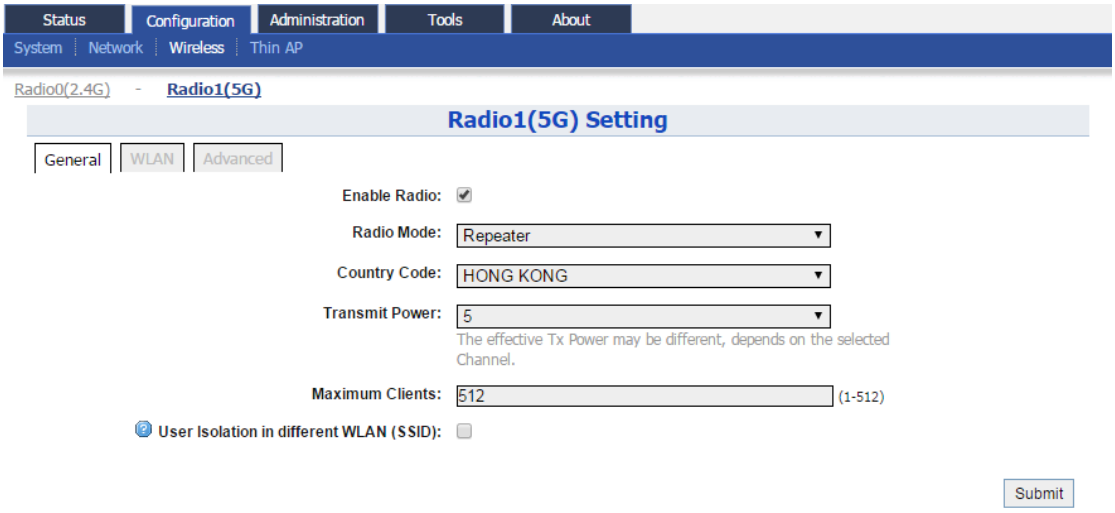


Figure 40 – Radio 1 General Setting of Repeater

1. Go to **Configuration** > **Wireless** > **Radio1(5G) > General;**
2. Select **Enable Radio** checkbox to enable radio interface
3. Select *Repeater* in **Radio Mode**
4. Change the following settings:
   Country Code – Select an option that matches your device's installation location; *Hong Kong* is the default setting.

Note:
- Country code sets the regulatory domain for maximum transmission power that Repeater can use

Transmission Power – Select the total transmission power for the radio interface.
Maximum Client – Specify the maximum associated client between *1* and *512* that the radio interface serves. *512* is the default setting.
Enable Inter-WLAN User Isolation - Select the checkbox to block the users' communication across different SSID in the AP directly.

5. Click **Submit**
6. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Repeater WLAN Configuration

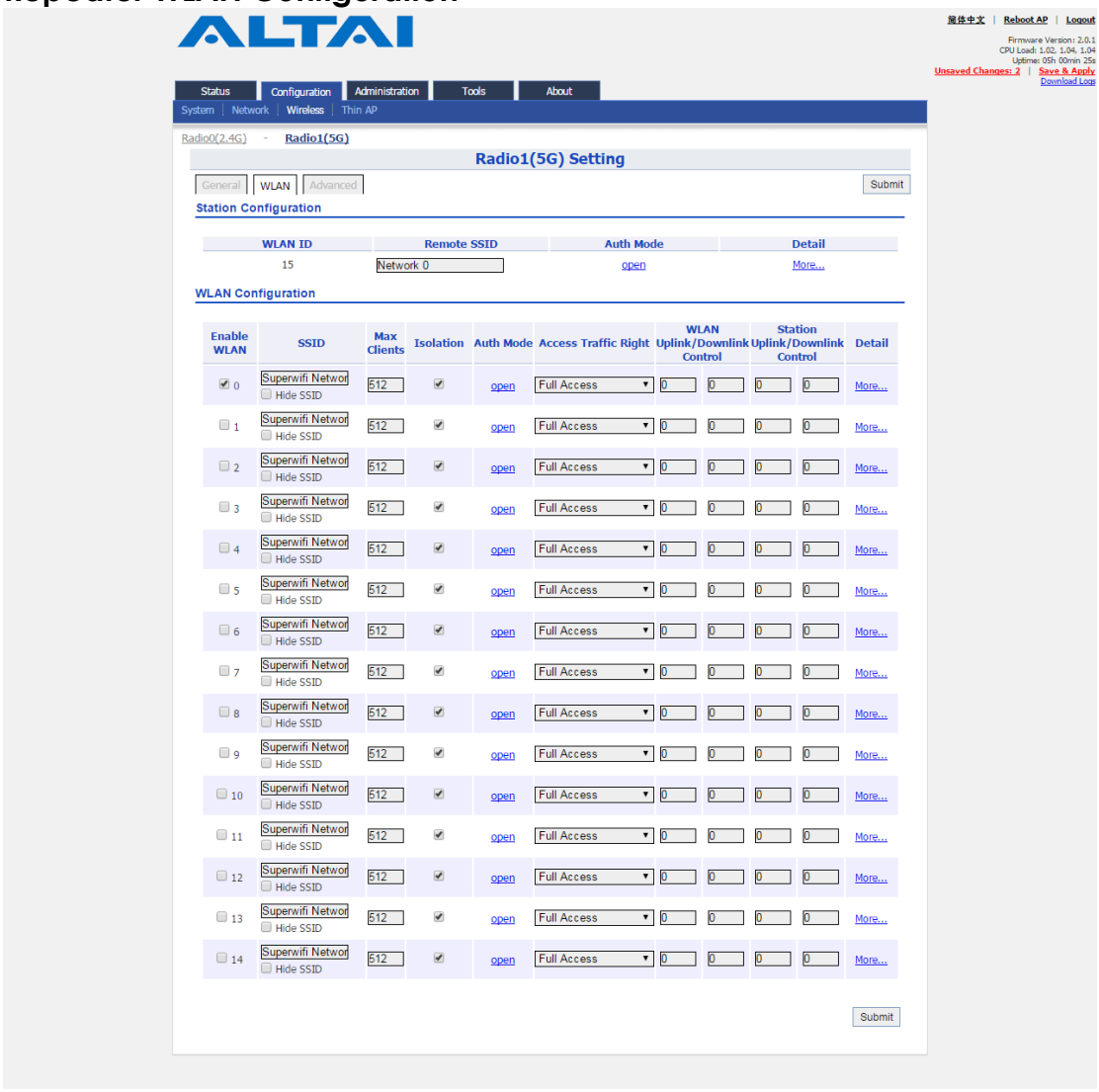


Figure 41 – WLAN List of Repeater

1. Go to **Configuration** > **Wireless** > **Radio1(5G)** > **WLAN** > **WLAN Configuration** > **WLAN 0-14** > **More…** for extending WLAN service form remote SSID.
2. Please refer to 4.1.3 on page 16 for **WLAN Configuration**.

Altai Technologies Ltd. All rights reserved

4.2. Advance Configurations

4.2.1. Assign a unique identification on AP for network management

If your network contains many AP, consider assigning a unique system info setting for each of them to facilitate network management.

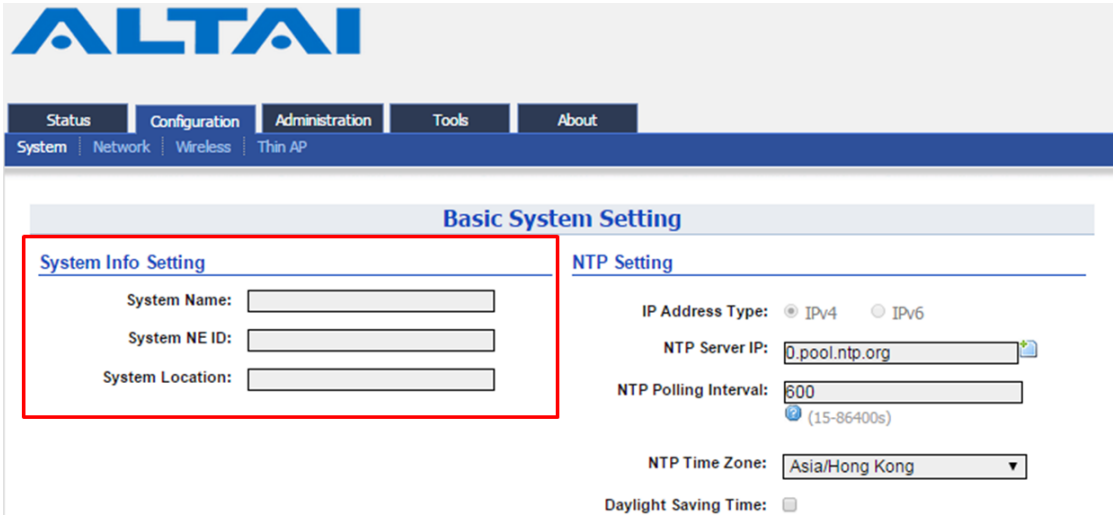


Figure 42 – Unique Identification on AP for Network Management

1. Click **Configuration** > **System**
2. Type in a string up to 255 characters in **System Name**
3. Type in a string up to 64 characters in **System NE ID**
4. Type in a string up to 255 characters in **System Location**
5. Click **Submit**
6. Click **Save & Apply**

4.2.2. Configure syslog settings

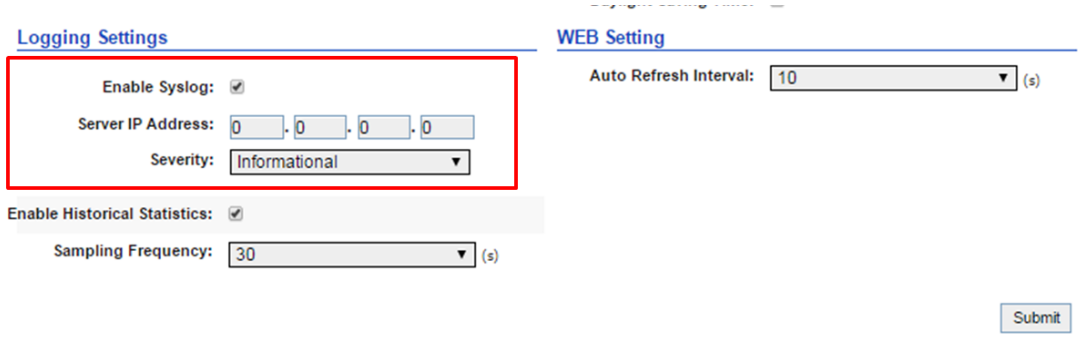


Figure 43 – Syslog Setting

1. Click **Configuration** > **System**
2. Change the following settings:

Altai Technologies Ltd. All rights reserved

Enable Syslog – Select the checkbox to enable system logging function
Server IP Address – Type in IP address of the remote syslog server that AP sends system logs instantaneously. *0.0.0.0 denote that AP saves the syslog in its local memory*
Severity – Set severity level of log that AP stores / sends to remote syslog server:

Emergency	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
Alert	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
Critical	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
Error	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
Warning	Warning messages, not an error, but indicate that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
Notice	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
Informational	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required. (Default Setting)
Debug	Info useful to developers for debugging the application, not useful during operations.

3. Click **Submit**
4. Click **Save & Apply**

4.2.3. Configure historical statistics settings

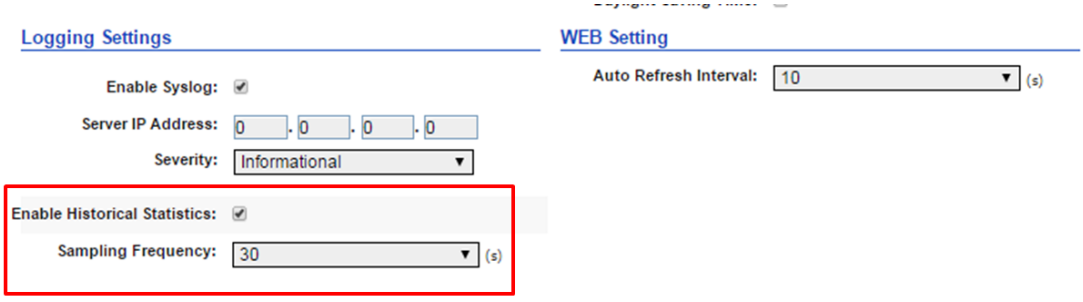


Figure 44 – Historical Statistic Setting

1. Click **Configuration** > **System**
2. Change the following settings:
   Enable Historical Statistics - Select the checkbox to enable AP statistics function

Altai Technologies Ltd. All rights reserved

Sampling Frequency - Set the sampling time of statistics:

1s	1 second per sample
5s	5 seconds per sample
10s	10 seconds per sample
30s	30 seconds per sample (Default Setting)

3. Click **Submit**
4. Click **Save & Apply**

4.2.4. Configure refresh interval of on-screen information on Web UI

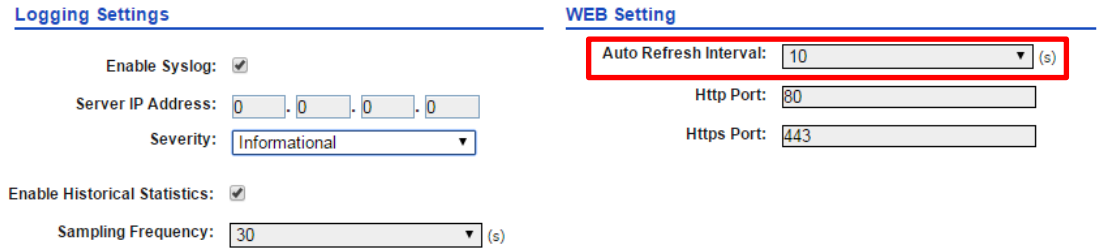


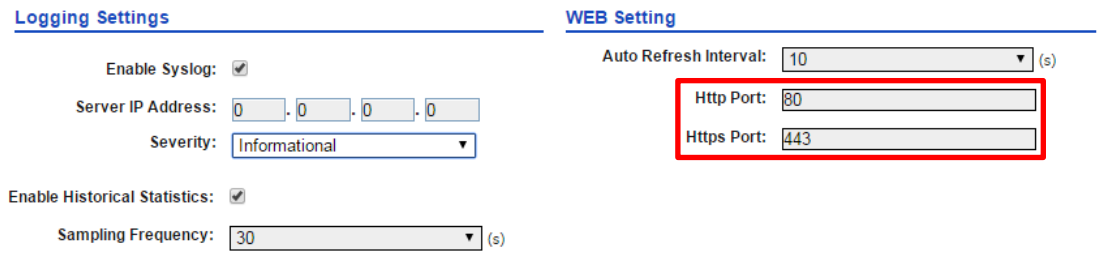
Figure 45 – Auto Refresh Interval Setting

1. Click **Configuration** > **System**
2. Change the following setting:
   Auto Refresh Interval - specify the interval in second that Web UI refreshes itself automatically:

Disable	Refresh manually
5s	Refresh every 5 seconds
10s	Refresh every 10 seconds (Default Setting)
20s	Refresh every 20 seconds
30s	Refresh every 30 seconds
40s	Refresh every 40 seconds

3. Click **Submit**
4. Click **Save & Apply**

4.2.5. Configure http and https port number



1. Click **Configuration** > **System**
2. Change the following setting:
   Http Port – specify the http port number. Default is port 80.
   Https Port – specify the https port number. Default is port 443.
3. Click **Submit**
4. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.2.6. Configure AP as IP Gateway

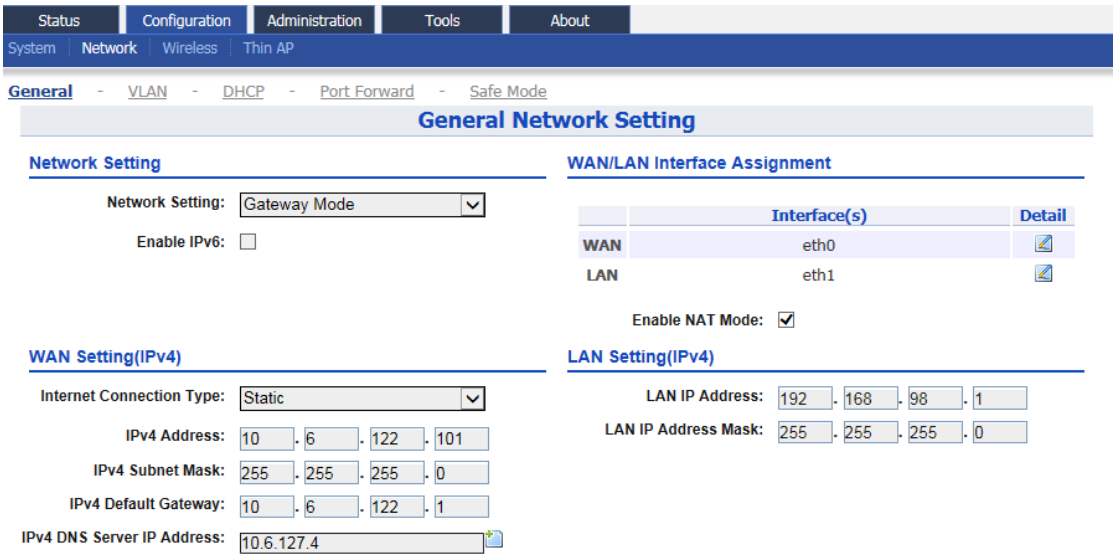


Figure 46 – Gateway Settings

1. Go to **Configuration** > **Network > General**
2. Select Gateway in **Network Setting**
3. Change the followings on **WAN setting**:
   Internet Connection Type – Set AP as a client with fixed IP address or DCHP client:
   Static Stand for Static IP addressing; AP will not update its IP address automatically
   DHCP Client Require an IP address from DCHP server on the network; AP renews its IP address periodically

   IPv4 Address – Type in an IP address for AP (Static Internet Connection Type only)
   IPv4 Subnet Mask – Type in a subnet mask for AP (Static Internet Connection Type only)
   IPv4 Default Gateway – Type in an IP address of default gateway for AP (Static Internet Connection Type only)
   IPv4 DNS Server – Type in one or more DNS server for AP (Static Internet Connection Type only).
4. Change the followings on **LAN setting**:
   LAN IP Address – Provide an IP address on LAN interface of device
   LAN IP Address Subnet Mask – Provide a subnet mask on LAN interface of device
5. Assign enabled interfaces into WAN group or LAN group in **WAN/LAN Interface Assignment**; all interfaces in the same group work as bridge
6. Select **Enable NAT Mode** to enable NAT in AP [Optional]
7. Click **Submit**
8. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.2.7. Enable Spanning Tree Protocol (STP)

Figure 47 – STP Setting

1. Go to **Configuration** > **Network > General > STP Setting**
2. Select Enable STP to enable spanning tree protocol on A8n (ac) device
3. Click **Submit**
4. Click **Save & Apply**

4.2.8. Configure the operating mode on Ethernet interface

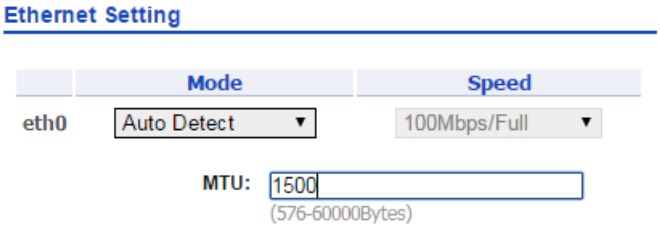


Figure 48 – Ethernet Setting

1. Go to **Configuration** > **Network > General > Ethernet Setting**
2. Change the following settings:
   Mode – Select the operating mode on Ethernet 0:

Auto	A8n (ac) device negotiates with connected device automatically and selects the best option
Manual	Network administrator select speed and duplex mode manually

   Speed (Eth0) – Select the speed and duplex mode on Ethernet 0. It is only available if *Manual* is selected in **Mode**:
   10Mbps/Half
   10Mbps/Full
   100Mbps/Half
   100Mbps/Full

   MTU – Select the Maximum transmission unit on Ethernet 0. Default is 1500 Bytes.

3. Click **Submit**
4. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.2.9. VLAN

VLAN is layer-2 network domain that may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers.

Note:
- *VLAN can be enabled on Switch mode ONLY*

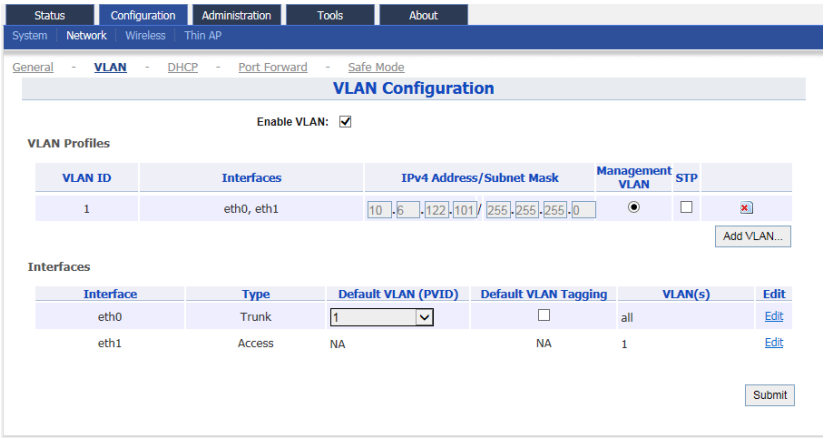


Figure 49 – VLAN Settings

Enable VLAN

1. Go to **Configuration** > **Network > VLAN**
2. Click **Submit**
3. Go to **Configuration** > **Network > VLAN > VLAN Profiles**

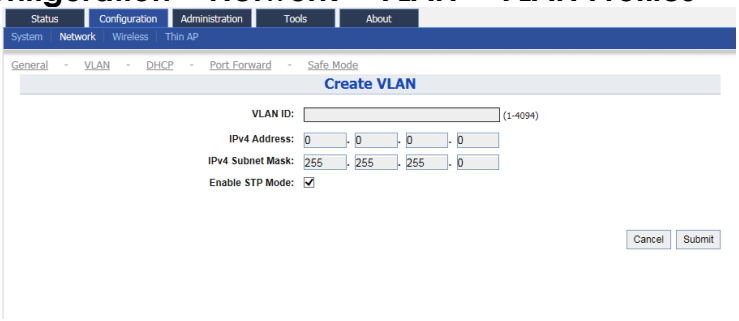


Figure 50 – VLAN Setting – Create VLAN

4. Click **Add VLAN** to create new VLAN
5. Change the following settings:
   VLAN ID – Type in an identification number that represents a VLAN
   IPv4 Address – Type in IP address for the VLAN
   IPv4 Subnet Mask - Type in subnet mask for the VLAN
   Enable STP Mode – Select the checkbox to enable STP on VLAN
6. Click **Submit**
7. Select a desired VLAN as **Management VLAN**
8. Click **Submit**

Altai Technologies Ltd. All rights reserved

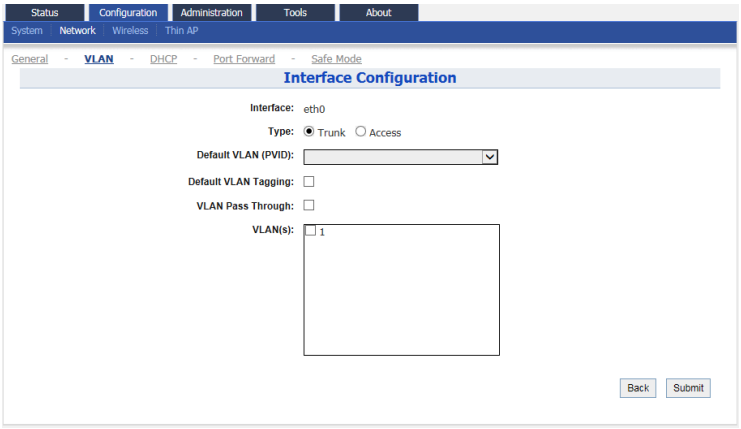


Figure 51 – VLAN Setting – Interface Configuration

9. Go to **Configuration** > **Network > VLAN > Interfaces**
10. Click Edit to assign VLAN profile on each interface respectively
11. Change the following settings:

Type – select type of VLAN connection link:

Trunk	Able to carry multiple VLAN traffic. Typically trunk link is used to connect switches to other switches or to routers
Access	It is part of only one VLAN; it is for end devices

If *Access* is selected on **Type;**

VLAN – assign the VLAN profile on the interface

If *Trunk* is selected on **Type;**

Default VLAN (PVID) - Stand for Port VLAN ID; select the default VLAN for the interface

Default VLAN Tagging – Select checkbox that AP tags the untagged packet with PVID

VLAN Pass Through - Select checkbox that AP does not modify the incoming packets that are tagged. Also, AP tags the packets, which are not tagged if **Default VLAN Tagging** is selected.

VLAN(s) – Assign one or more VLAN profile to the interface. Unlike VLAN Pass Trough, the interface only forwards the packets to selected VLAN.

12. Click **Submit**
13. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.2.10. DHCP

A8n (ac) series products have built-in DHCP server; it can dynamically distribute network configuration parameters to the connected end devices on all LAN interfaces.

Note:

- *DHCP server is available on Gateway mode ONLY*

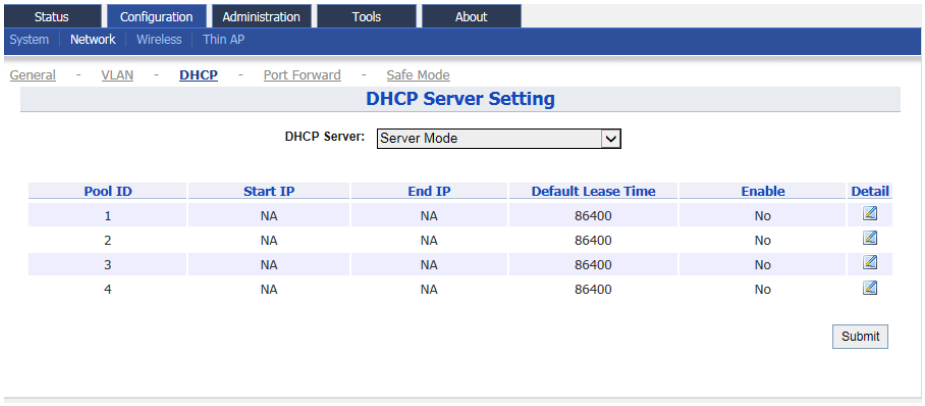


Figure 52 – DHCP Server Setting

Enable DHCP server

1. Go to **Configuration** > **Network > DHCP**
2. Select *Server Mode* on **DHCP Server**
3. Click **Submit**
4. Click  under **Detail** of each pool

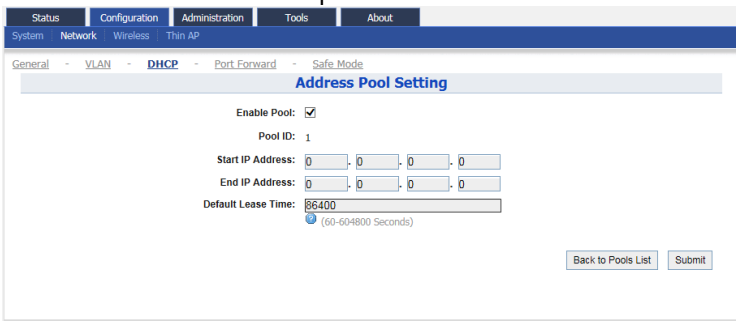


Figure 53 – DHCP Server – Address Pool Setting

5. Select **Enable Pool** check box
6. Type in IP address on **Start IP Address**
7. Type in IP address on **End IP Address**
8. Specify lease time between *60s* and *604800s* in **Default Lease Time**; *86400s* is default setting
9. Click **Submit**
10. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.2.11. Port Forward

Port forward allows remote computers from WAN to connect to a specific computer or service within a private local-area network (LAN).

Note:
- *Port forward is available on Gateway mode ONLY*

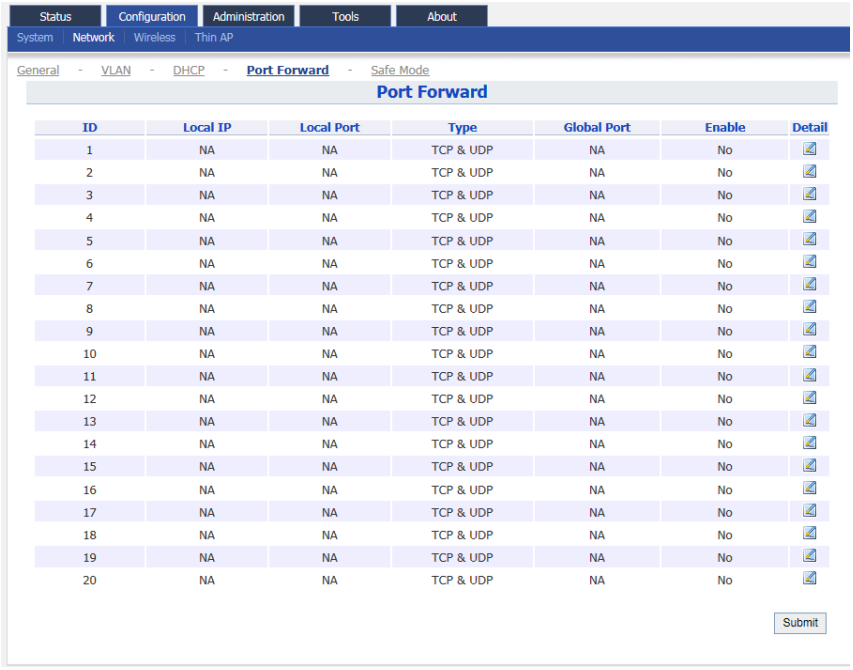


Figure 54 – Port Forward List

Enable port forward on A8n (ac) device

1. Go to **Configuration** > **Network > Port Forward**

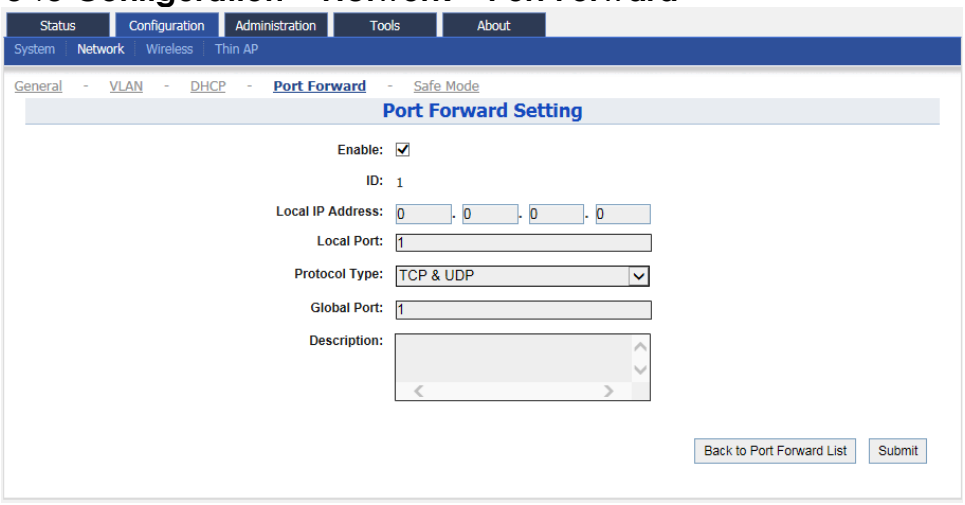


Figure 55 – Port Forward Setting

2. Click  under **Detail**
3. Select **Enable** checkbox
4. Type in target host's IP address in **Local IP Address**
5. Type in port number of target host in **Local Port**

Altai Technologies Ltd. All rights reserved

6. Select suitable protocol in **Protocol Type**:
   TCP & UDP
   TCP
   UDP
7. Type in port number of AP in **Global Port**
8. Type in description in **Description** [Optional]
9. Click **Submit**
10. Click **Save & Apply**

4.2.12. Safe Mode

Safe Mode is for detecting the backhaul link integrity. If the AP loses its backhaul connectivity, it forces the clients to re-associate with another AP by changing its SSID to a default Safe Mode_X, where X is the MAC address of the radio interface in hexadecimal.
This action can protect the client from connecting to the AP which has no backhaul to the Internet end. Total duration for AP from losing backhaul link to safe mode is 3 x ping interval seconds.

Note:
- A8n (ac) recovers itself from safe mode if it detects the backhaul link is recovered

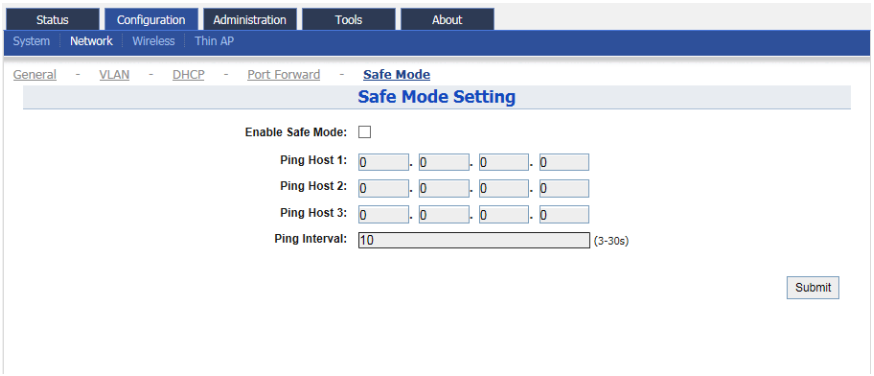


Figure 56 – Safe Mode Setting

Enable safe mode on A8n (ac) device

1. Go to **Configuration** > **Network > Safe Mode**
2. Select **Enable Safe Mode** checkbox
3. Type in at least one IP address of remote host in **Ping Host 1 / Ping Host 2 / Ping Host 3**
4. Type in interval time between 3s and 30s in **Ping Interval**
5. Click **Submit**
6. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

4.2.13. Advanced Settings on Radio Interface

A8n (ac) provides advanced settings on each radio interface; these settings include data rate, AirFi, Tx/Rx Stream settings … etc.

Caution:

- Inappropriate configuration may bring negative impact on the network performance
- It is not suggested to change the parameters in Advanced Radio Settings unless you are experienced administrators.
- ***Default setting is recommended***

Figure 57 – Radio 0's Advanced Settings

Altai Technologies Ltd. All rights reserved

Advanced Settings

Configure AMPDU and AMSDU on radio interface

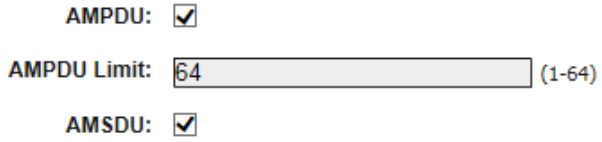


Figure 58 – AMPDU and AMSDU Setting

1. 2.4G Radio: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Radio: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Select **AMPDU** checkbox to enable aggregation of MAC protocol unit
3. Type in the maximum number of data frame between *1* and *64* that A8n (ac) pushes them into single PPDU; *64* is default setting
4. Select **AMSDU** checkbox to enable aggregation of MAC service data unit; A8n (ac) pushes aggregated MSDU (MAC service data units) into a single MPDU
5. Click **Submit**
6. Click **Save & Apply**

Configure the number of transmit radio chains and receive radio chains

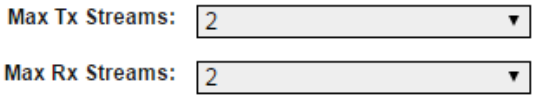


Figure 59 – transmit radio chains and receive radio chains setting

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Select the maximum number of transmission between *1* and *2* on **Max Tx Streams**
3. Select the maximum number of transmission between *1* and 2 on **Max Rx Streams**
4. Click **Submit**
5. Click **Save & Apply**

Configure beacon interval of BSS

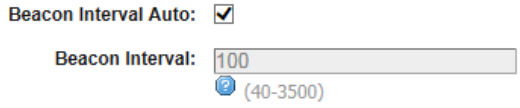


Figure 60 – Beacon Setting

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**

Altai Technologies Ltd. All rights reserved

2. Change the following settings:
   Beacon Interval Auto – Select checkbox that A8n (ac) tunes the interval of beacon transmissions of each supported BSS automatically
   Beacon Interval – Available if **Beacon Interval Auto** is NOT selected; Specify the interval time between *40*ms and *3500*ms in **Beacon Interval.** Each BSS share this setting.
3. Click **Submit**
4. Click **Save & Apply**

Configure Delivery Traffic Indication Message (DTIM) time

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Specify the interval time between *1* and *255* in **DTIM.**
3. Click **Submit**
4. Click **Save & Apply**

Note:
- The higher the DTIM period, the longer a client device may sleep and therefore the more power that particular client device may potentially save.

Modify protect mechanism on hidden node problem of Wi-Fi network

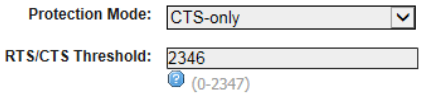


Figure 61 – Protection Mechanism Setting

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Select suitable mechanism on **Protection Mode**; you can select:
   None - no protect mechanism is used. It is the default setting.
   CTS-only - also known as CTS-to-Self; AP issues a CTS frame to itself before sending data. All clients will not transmit during the time.
   RTS-CTS - AP sends a RTS frame, waits for the clients CTS frame and then sends the data packet. It allow more robust operation, but at the expense of additional overheads.
3. Specify frame size in byte between *0* and *2347* bytes on **RTS/CTS Threshold**; *2346* is default setting.
   If a frame is smaller than the RTS/CTS threshold, it will be sent by the AP without modification. If a frame is larger than the RTS/CTS threshold, then two frames will be sent by the AP. The first frame is an RTS (request to send) frame. After the RTS frame is sent, the AP listens

Altai Technologies Ltd. All rights reserved

for the corresponding CTS from the target client. Upon reception of the CTS, the AP then sends the data frame. There are trade-offs when considering what value you should set for the RTS/CTS threshold. Smaller values will cause RTS to be sent more often, increasing overheads. However, the more often RTS packets are sent, the sooner the system can recover from collisions. It is recommended to use the default value or only minor reductions of the default setting.

4. Click **Submit**
5. Click **Save & Apply**

Change distance setting on A8n (ac)

Distance setting is the estimated distance of target area (round to the nearest km); A8n (ac) adjusts the round-trip time latency according to this setting.

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Type in the estimate distance of target area between 1 and 50 km in **Distance**; 2 km is default setting.
3. Click **Submit**
4. Click **Save & Apply**

Enable IGMP Snooping

AP is a Layer 2 device when it is configured as Switch mode. However, IGMP Snooping implementation on AP is a little bit different than that of standard Layer 2 Switch.

Each Virtual AP (WLAN) port is similar to a Layer 2 switch port. With IGMP Snooping enabled in the AP, clients associated to a VAP will only receive multicast packets if there is at least one client joined the multicast group in that VAP. Unlike ordinary IGMP Snooping implementation, where Layer 2 switch converts multicast to unicast and delivers them to devices registered with the multicast group, AP should simply send out the multicast packets from the VAP which has at least one client joined the multicast group. This is done because the wireless media is a broadcast media. It does not need to be sent multiple times when there are more than one registered clients.

When IGMP Snooping is turned on, multicast packets should be dropped at the VAP exit if there is no client from the VAP who has joined the corresponding multicast group.

The IGMP snooping forwarding table (port and multicast MAC address mapping table) should support aging mechanism to age out the entry which has no multicast traffic for a period of time.

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**

Altai Technologies Ltd. All rights reserved

5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**

2. Select **IGMP Snooping** checkbox to enable IGMP Snooping
3. Click **Submit**
4. Click **Save & Apply**

Enable multicast traffic

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Select **Multicast Traffic** checkbox that A8n (ac) process multicast traffic in all WLANs; otherwise; AP drops the multicast traffic.
3. Click **Submit**
4. Click **Save & Apply**

Enable Nearby AP List on A8n (ac)

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
   5G Interface: Go to **Configuration** > **Wireless > Radio1 > Advanced > Advanced Settings**
2. Select **Nearby AP List** checkbox that A8n (ac) sniffs the surrounding AP periodically
3. Click **Submit**
4. Click **Save & Apply**

AirFi Settings

AirFi technology is an advanced software control wireless algorithm developed by Altai for optimizing network throughput capacity performance. Using the Altai AirFi control algorithm can optimize the wireless bandwidth for the high speed clients as well as the low speed clients (i.e. 11b and 11g clients), and as a result the system throughput can be improved substantially.

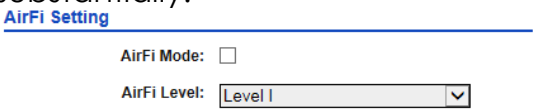


Figure 62 – AirFi Setting

1. Go to **Configuration** > **Wireless > Radio0 > Advanced > Advanced Settings**
2. Select **AirFi** checkbox to enable AirFi feature
3. Select suitable level in **AirFi Level**
   Level I - favor the fast (802.11n) client most
   Level I - favor the fast (802.11n) client moderate
   Level III - favor the fast (802.11n) client less
4. Click **Submit**
5. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

Note:
- Level I is recommended

Data Rate Setting

Altai AP provides the capability to limit all clients to transmit data and multicast data in the certain data rate.

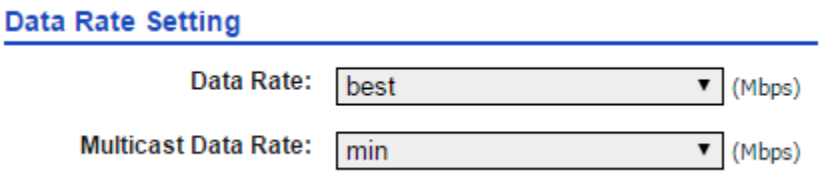


Figure 63 – Data Rate Setting

Note:
- Data rate: Best and Multicast Data Rate: Min is recommended

1. 2.4G Radio: Go to **Configuration** > **Wireless > Radio0 > Advanced > Data Rate Settings**
   5G Radio: Go to **Configuration** > **Wireless > Radio1 > Advanced > Data Rate Settings**
2. Select a data rate on **Data Rate**; *best* is default setting
3. Select a data rate on **Multicast Data Rate**; *min* is default setting
4. Click **Submit**
5. Click **Save & Apply**

4.2.14. Quality of Service on Radio Interface

A8n (ac) provides QoS/WMM configuration on both radio interface and each WLAN.

Modify the QoS setting on Radio

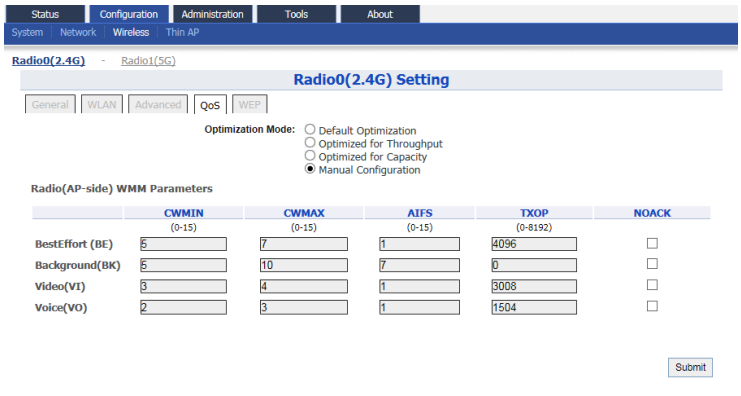


Figure 64 – QoS Setting on Radio

1. 2.4G Interface: Go to **Configuration** > **Wireless > Radio0 > QoS**

Altai Technologies Ltd. All rights reserved

5G Interface: Go to **Configuration** > **Wireless > Radio1 > QoS**

2. Select suitable configuration in **Optimization Mode**; you can select:
   Default Optimization – a set of QoS/WMM parameters for most scenarios; it is a default setting
   Optimized for throughput – a set of QoS/WMM parameters for single user Wi-Fi network; Wi-Fi network achieves the highest throughput for a single user.
   Optimized for capacity - a set of QoS/WMM parameters for multi-user (>20) Wi-Fi network; Wi-Fi network can achieve highest system throughput for multiple users
   Manual Configuration – Specify QoS/WMM parameters manually
3. Click **Submit**
4. Click **Save & Apply**

Modify the QoS setting in WLAN 0 – 15

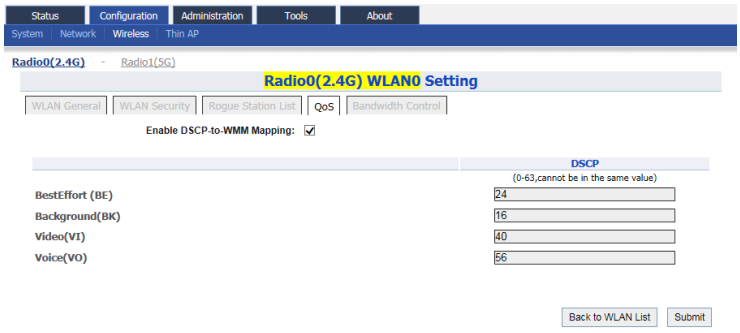


Figure 65 – QoS Setting on WLAN 0-15

1. 2.4G WLAN 0-15: Go to **Configuration** > **Wireless > Radio0 > WLAN 0-15 > QoS**
   5G WLAN 0-15: Go to **Configuration** > **Wireless > Radio1 > WLAN 0-15 > QoS**
2. Specify QoS/WMM parameters manually
3. Click **Submit**
4. Click **Save & Apply**

4.2.15. Bandwidth Control on WLAN

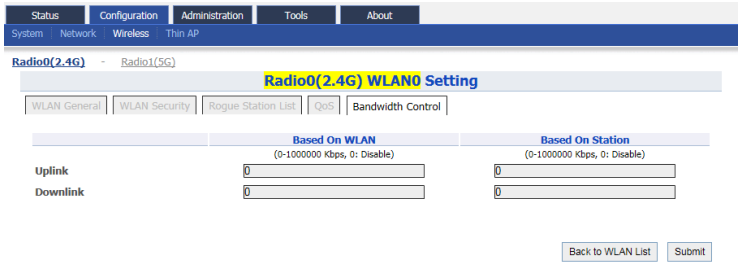


Figure 66 – Bandwidth Control Setting on WLAN 0-15

Altai Technologies Ltd. All rights reserved

Enable bandwidth control for the WLAN on WLAN 0 – 15

1. 2.4G WLAN 0-15: Go to **Configuration** > **Wireless > Radio0 > WLAN 0-15 > Bandwidth Control**
   5G WLAN 0-15: Go to **Configuration** > **Wireless > Radio1 > WLAN 0-15 > Bandwidth Control**
2. Type in maximum throughput in kbps between *0* to *1000000* kbps on **Uplink** under **Based on WLAN;** *0* denotes disable, and is default setting
3. Type in maximum throughput in kbps between *0* to *1000000* kbps on **Downlink** under **Based on WLAN**; *0* denotes disable, and is default setting
4. Click **Submit**
5. Click **Save & Apply**

How to enable bandwidth control per station on WLAN 0 – 15

1. 2.4G WLAN 0-15: Go to **Configuration** > **Wireless > Radio0 > WLAN 0-15 > Bandwidth Control**
   5G WLAN 0-15: Go to **Configuration** > **Wireless > Radio1 > WLAN 0-15 > Bandwidth Control**
2. Type in maximum throughput in kbps between *0* to *1000000* kbps on **Uplink** under **Based on Station;** *0* denotes disable, and is default setting
3. Type in maximum throughput in kbps between *0* to *1000000* kbps on **Downlink** under **Based on Station**; *0* denotes disable, and is default setting
4. Click **Submit**
5. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

5.Manage Your Access Point

5.1. User Admin

A8n (ac) device allows network administrator to manage user account and privilege for accessing Web UI via local authentication and/or RADIUS authentication.

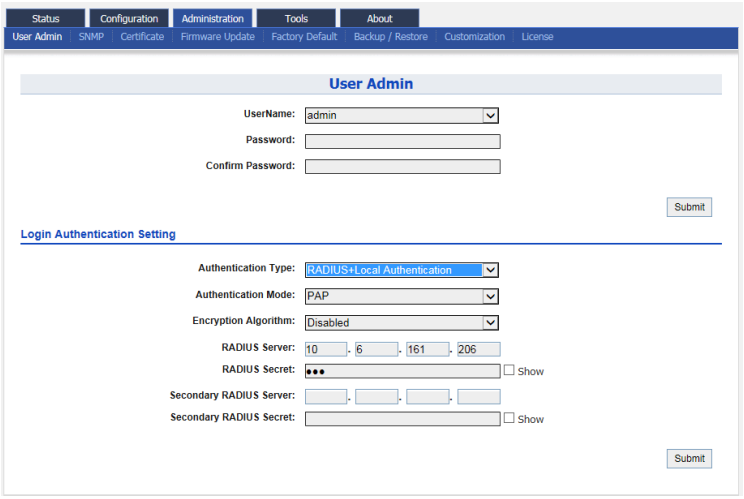


Figure 67 – User Admin

Table 4 describes the authentication setting of A8m (ac) device.

Authentication	Description
Local (Default)	Support 3-level User Login (root/admin/guest)
RADIUS	Authenticate user through RADIUS; if no response returned from RADIUS server, AP fallbacks to local authentication
RADIUS + Local	Login AP with local user login or RADIUS user login

Table 4 - Different authentication type

5.1.1. Local authentication

Modify admin account's password

1. Go to **Administration** > **User Admin**
2. Select *admin* in **UserName**
3. Type a new password in **Password**
4. Type a new password again in **Confirm Password**
5. Click **Submit**

Modify guest account's password

1. Go to **Administration** > **User Admin**
2. Select *guest* in **UserName**

Altai Technologies Ltd. All rights reserved

3. Type a new password in **Password**
4. Type a new password again in **Confirm Password**
5. Click **Submit**

Note:
- Please login as admin for modifying password

5.1.2. RADIUS authentication

Enable RADIUS authentication in A8n (ac) products

1. Go to **Administration** > **User Admin > Login Authentication Setting**
2. Select *RADIUS authentication* or *RADIUS + Local authentication* in **Authentication Type**
3. Select suitable authentication in **Authentication Mode;** you can select:
   PAP
   EAP
4. Select suitable encryption in **Encryption Algorithm;** you can select:
   For authentication Mode is *PAP:*
   Disable
   For authentication Mode is *EAP:*
   PEAP-GTC
   PEAP-MS-CHAP-V2
   TTLS-PAP
   TTLS-CHAP
   TTLS-MS-CHAP
   TTLS-MS-CHAP-V2
5. Provide IP address of remote RADIUS server in **RADIUS Server**
6. Provide suitable secrets in **Secret** of **RADIUS Secret.**
7. Left **Secondary RADIUS Server** blank if no backup RADIUS server is available
8. Left **Secondary RADIUS Secret** blank if no backup RADIUS server is available
9. Click **Submit**
10. Click **OK** (see Figure 68)

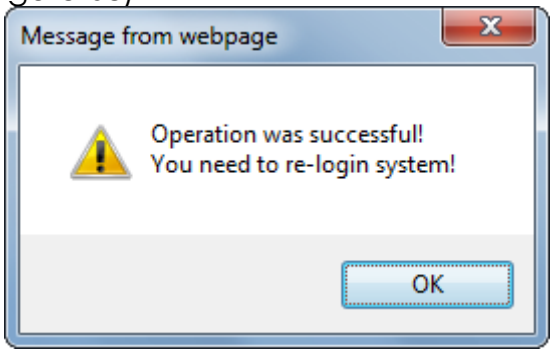


Figure 68 – Popup window for confirming the change of RADIUS authentication

Altai Technologies Ltd. All rights reserved

5.2. SNMP

Simple Network Management Protocol (SNMP) is a Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

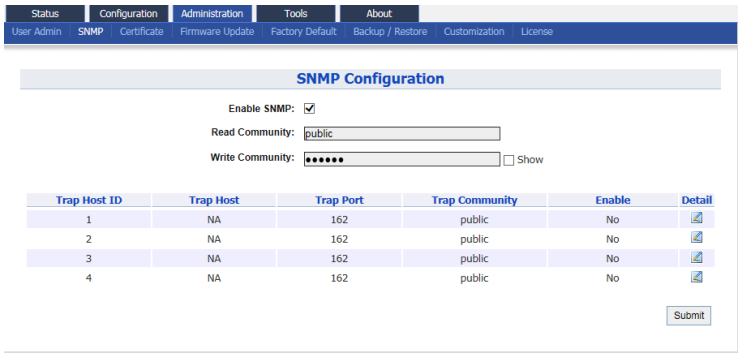


Figure 69 – SNMP Configuration

5.2.1. Enable SNMP in A8n (ac) products

1. Go to **Administration** > **User Admin > SNMP**
2. Select **Enable SNMP** checkbox to enable SNMP function
3. Type in suitable string in **Read Community**; the string of **Read Community** between Network Manage System (NMS) and A8n (ac) must be identical, otherwise, NMS cannot get information from A8n (ac). *public* is default setting.
4. Type in suitable string in **Write Community**; the string of **Write Community** between Network Manage System (NMS) and A8n (ac) must be identical, otherwise, NMS cannot modify A8n (ac)'s setting. *netman* is default setting.
5. Click **Submit**
6. Click **Save & Apply**

Note:

- A8n (ac) support up to four trap host at the same time. The information about trap hosts will be listed in the trap host table (see Figure 70)

Trap Host ID	Trap Host	Trap Port	Trap Community	Enable	Detail
1	NA	162	public	No	
2	NA	162	public	No	
3	NA	162	public	No	
4	NA	162	public	No	

Figure 70 – Trap host table

Altai Technologies Ltd. All rights reserved

5.3. Certificate

A8n (ac) devices support both HTTP and HTTPS connection for their web UI. Certificate management allows network administrator to upload their own certifications for HTTPS connection.

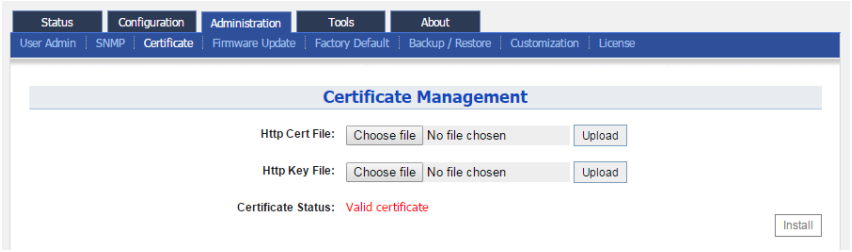


Figure 71 – Certificate Management

5.3.1. Upload the customized certification for HTTPS connection on A8n (ac) products

1. Go to **Administration** > **Certificate**
2. Click **Choose file** on **Http Cert File** and select suitable certification file for HTTPS connection
3. Click **Upload** on **Http Cert File** to upload certification
4. Click **Choose file** on **Http Key File** and select suitable certification file for HTTPS connection
5. Click **Upload** on **Http Key File** to upload certification
6. Click **Install**

Note:

- The existing certification file and key file will be overwritten for executing installation each time

Altai Technologies Ltd. All rights reserved

5.4. Firmware Update

Network administrator updates (upgrades or downgrades) A8n (ac) device's firmware via web UI.

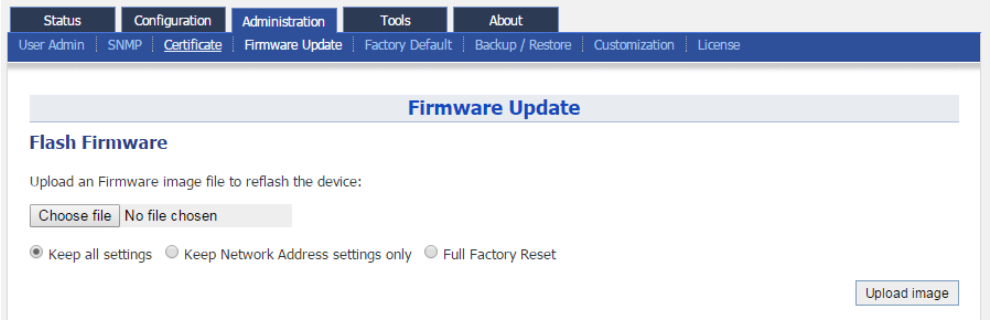


Figure 72 – Firmware Update

5.4.1. Update A8n (ac) device's firmware

1. Go to **Administration** > **Firmware Update**
2. Click **Choose file**, then select suitable firmware image file (.bin)
3. You may select:

Keeps all settings	Device keeps all operating setting after updating firmware
Keep Network Address settings only	Device keeps IP address, subnet mask only after updating firmware; the other settings will be restored as default settings
Full Factory Reset	Device restores all setting as default settings after updating firmware

4. Click **Upload Image**
5. If uploaded firmware image is valid, click **Proceed** to continue; otherwise, error message will be shown
6. Wait unit A8n (ac) completes updating firmware
7. Login with correct username and password, then check the firmware version on **About** > **Software Version**

Caution:

- **Do not interrupt the process of firmware update. Please maintain network connection and power supply during updating firmware; otherwise A8n (ac) may not function.**

Altai Technologies Ltd. All rights reserved

5.5. Factory Default

Network administrator restores A8n (ac) device's settings as default settings via web UI.

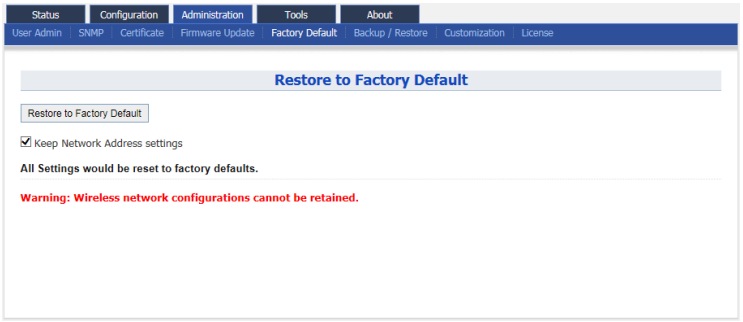


Figure 73 – Restore to Factory Default

5.5.1. Restore A8n (ac) device's settings with default settings

1. Go to **Administration** > **Factory Default**
2. Select **Keep Network Address settings** checkbox for keeping IP address and subnet mask settings; otherwise, deselect the checkbox
3. Click **Restore to Factory Default**

Note:

- Please refer to 2.3 Login the AP (via Ethernet) on page 4 for logging in A8n (ac) after performing factory default

5.6. Backup/Restore

Network administrator backups / restores A8n (ac) device's settings via web UI.

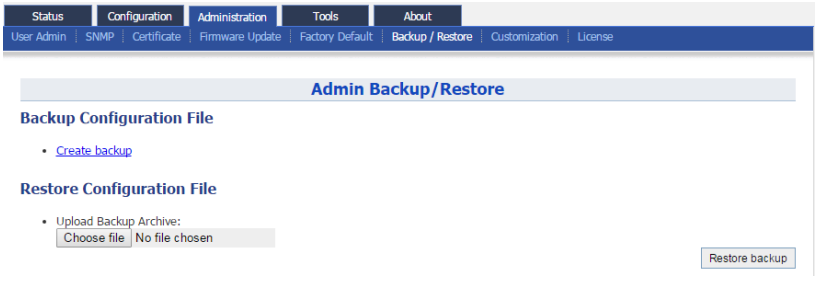


Figure 74 – Admin Backup / Restore

5.6.1. Backup A8n (ac) device's settings

1. Go to **Administration** > **Backup/Restore > Backup Configuration File**
2. Click Create backup and save configuration file

Altai Technologies Ltd. All rights reserved

5.6.2. Restore A8n (ac) device's settings with configuration file

1. Go to **Administration** > **Backup/Restore > Restore Configuration File**
2. Click **Choose file**, then select suitable configuration file (.tar.gz)
3. Click **Restore backup**

5.7. Customization

Network administrator may create customized settings as factory default settings for A8n (ac) products. Once the customized configuration file is imported, A8n (ac) products restore with the customized settings as default settings rather than the original default settings.

Figure 75 – Default Configuration Customization

5.7.1. Create customized configuration file for A8n (ac) products

1. Go to **Administration** > **Customization > Default Configuration Customization**
2. Click Product Customization Template to download configuration template file (.tar.gz)
3. Use 7-zip software to open the template file, and edit the files in the factory_default.zip.
4. Edit system, network, and wireless files with the desired settings;

system	Contain settings about SNMP, syslog …etc
network	Contain network settings about all interfaces, such as IP address, VLAN enabling, and STP …etc.
wireless	Contain settings about radio interfaces, including radio enabling, WLAN settings … etc

5. Save the modified files

Altai Technologies Ltd. All rights reserved

6. Go to **Administration** > **Customization** > **Default Configuration Customization**
7. Click **Choose file**, then select the modified customization file
8. Click **Install**

Caution:

- **Do not unzip the file during edit; otherwise, error may appear after uploading the customization file. 7-zip is recommended software to use in customization.**

Note:

- Customization will take effect after reboot. Since improper customization may cause malfunction of A8n (ac), please contact Altai support team (support@altaitechnologies.com) for any queries.

Altai Technologies Ltd. All rights reserved

6.Monitor Your Access Point

This chapter introduces various information / statistics from Web UI or LED indication that monitoring the device's status.

6.1. LED Colors and What They Mean

6.1.1. A8n (ac) series

LED	LED Status (Color)	Meaning
Power LED	Off	Power off
	Solid (Green)	Operating
Ethernet LED	Off	Link Down
	Solid (Green)	Link Up
	Blinking (Green)	Activity
Remarks: 1. **All LED will be off once pressing down the reset button** 2. **Pressing and holding the reset button until Power LED blinks once, the device reboots.** 3. **Pressing and holding the reset button until Power LED blinks twice consecutively, the device restores the factory default setting.**		

Table 5 – A8n (ac) series operation LED indicators

Altai Technologies Ltd. All rights reserved

6.2. Status > Overview

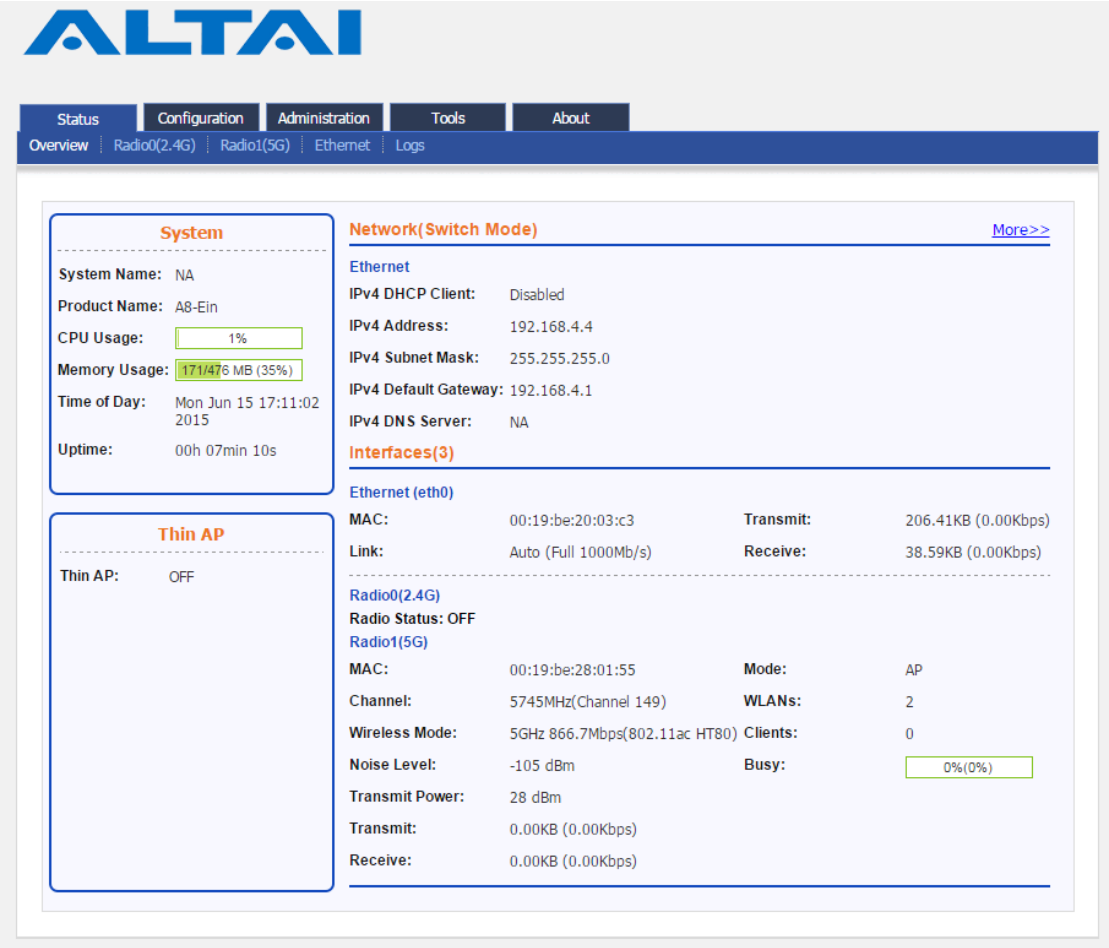


Figure 76 – A8n (ac) device's status overview

Status overview provides vital information on the device's status. Information includes system status, thin AP status, network status, and interfaces status.

6.2.1. System status

System status provides basic information and real time status of device.

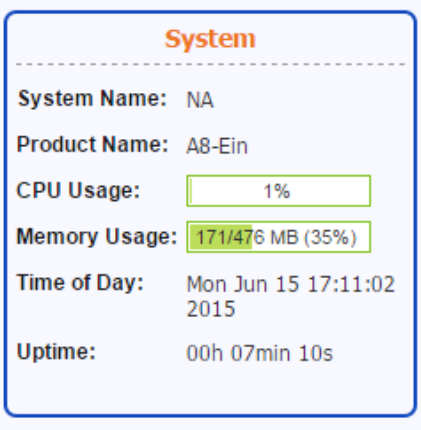


Figure 77 – System Status

Altai Technologies Ltd. All rights reserved

System Name – Name represents the device in Wi-Fi network; it is customized by network administrator.
Product Name – Device's product name
CPU Usage – indicate that how many CPU resources the device is currently using
Memory Usage – indicate that how many memory resources the device is currently using
Time of Day – system time of device
Uptime – indicate operation time of device from last time boot up / reboot

6.2.2. Thin AP

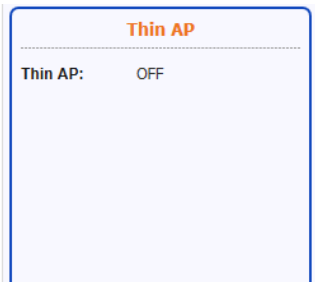


Figure 78 – Thin AP Status

Thin AP - indicate status of thin AP feature

6.2.3. Networks

Networks provide basic information about Layer 3 status.

Switch Mode

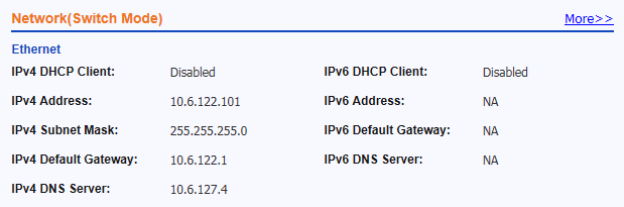


Figure 79 – Network Status in Switch Mode

IPv4 DHCP Client – indicate whether device's IP address is assigned by DHCP server or not
IPv4 Address – Current IPv4 address of device
IPv4 Subnet Mask – indicate the subnetwork device belongs to
IPv4 Default Gateway – indicate a node that helps device to another network.
IPv4 DNS Server - indicate a node that provides DNS service for the device

The following information is available if IPv6 option is enabled.
IPv6 DHCP Client – indicate whether device's IP address is assigned by IPv6 DHCP server or not
IPv6 Address – Current IPv6 address of device

Altai Technologies Ltd. All rights reserved

IPv6 Default Gateway – indicate a node that helps device to another network.
IPv6 DNS Server - indicate a node that provides DNS service for the device

Gateway Mode

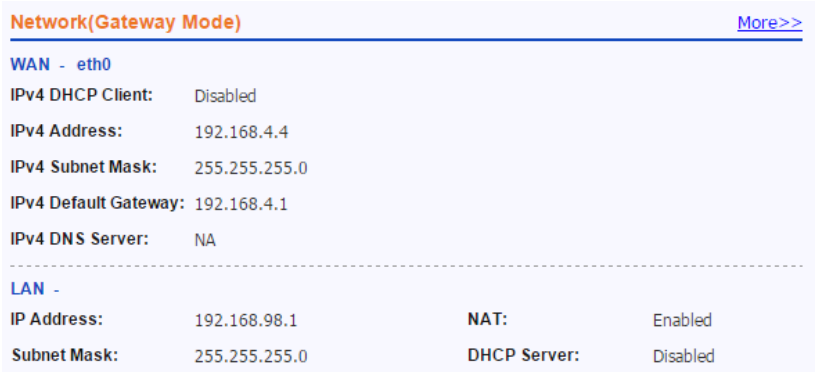


Figure 80 – Network Status in Gateway Mode

WAN
IPv4 DHCP Client – indicate whether device's IP address is assigned by DHCP server or not
IPv4 Address – Current IPv4 address of device on WAN
IPv4 Subnet Mask – indicate the subnetwork device belongs to
IPv4 Default Gateway – indicate a node that helps device to another network.
IPv4 DNS Server - indicate a node that provides DNS service for the device

LAN
IP Address - Current IP address of device on LAN
Subnet Mask – indicate the subnetwork device belongs to
NAT – indicate whether device performs network address translation (NAT) or not
DHCP Server - indicate whether built-in DHCP server is enabled or not

Altai Technologies Ltd. All rights reserved

6.2.4. Interfaces

Interfaces provide the real time status of all interfaces on the A8n (ac) device.

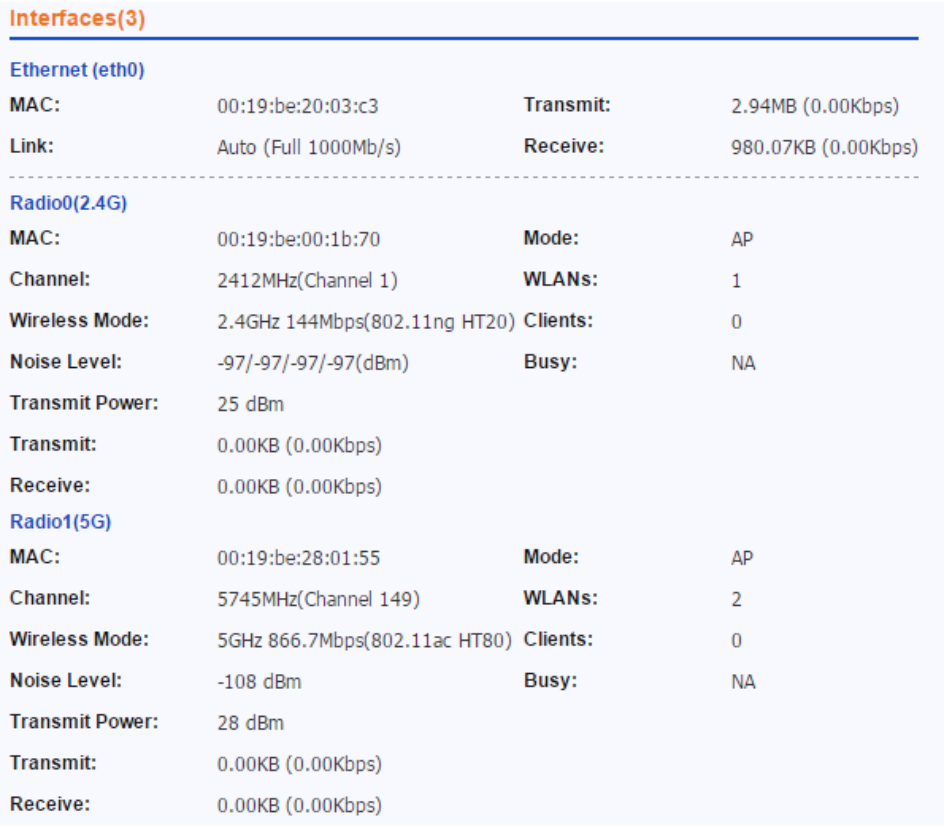


Figure 81 – Status of all available interfaces

Ethernet (eth0)

Figure 82 – Ethernet 0 Status

MAC – MAC address of Ethernet 0 interface
Link – indicate the status and operating mode of Ethernet 0
Transmit – indicate the traffic and instant throughput of transmission on Ethernet 0
Receive – indicate the traffic and instant throughput of receive operation on Ethernet 0

Altai Technologies Ltd. All rights reserved

Radio0 (2.4G)

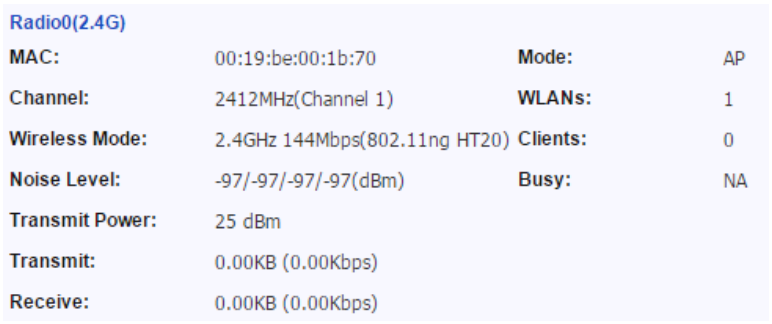


Figure 83 – Radio 0 Status

MAC – MAC address of Radio 0 interface
Channel – indicate operating frequency (channel) of Radio 0
Wireless Mode – indicate 802.11 standards that Radio 0 operates
Noise Level – indicate the noise level in terms of dBm of operating channel
Transmission Power – indicate the total transmission power of Radio 0
Transmit – indicate the traffic and instant throughput of transmission on Radio 0
Receive – indicate the traffic and instant throughput of receive operation on Radio 0
Mode – indicate operating mode of Radio 1
WLANs - indicate the number of operating WLAN on Radio 0 (AP mode and Repeater Mode only)
Clients - indicate the number of clients that Radio 0 servers currently (AP mode and Repeater mode only)
Connection – indicate connection status between Radio 0 and remote AP (Station mode only)
AP SSID – indicate the SSID that station associates with (Station mode only)
AP SNR – indicate received SNR from remote AP (Station mode only)
Busy – indicate busy of operating channel

Radio1 (5G)

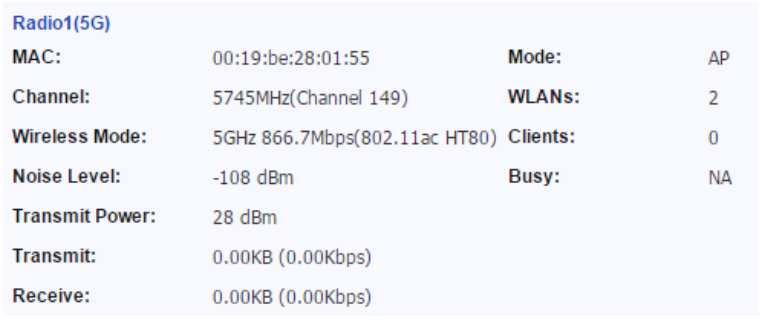


Figure 84 – Radio 1 Status

MAC – MAC address of Radio 1 interface
Channel – indicate operating frequency (channel) of Radio 1
Wireless Mode – indicate 802.11 standards that Radio 1 operates

Altai Technologies Ltd. All rights reserved

Noise Level – indicate the noise level in terms of dBm of operating channel
Transmission Power – indicate the total transmission power of Radio 1
Transmit – indicate the traffic and instant throughput of transmission on Radio 1
Receive – indicate the traffic and instant throughput of receive operation on Radio 1
Mode – indicate operating mode of Radio 1
WLANs - indicate the number of operating WLAN on Radio 1 (AP mode and Repeater Mode only)
Clients - indicate the number of clients that Radio 1 servers currently (AP mode and Repeater mode only)
Connection – indicate connection status between Radio 0 and remote AP (Station mode only)
AP SSID – indicate the SSID that station associates with (Station mode only)
AP SNR – indicate received SNR from remote AP (Station mode only)
Busy – indicate busy of operating channel

6.3. Status > Radio0(2.4G)

6.3.1. Status > Radio0(2.4G) > Status

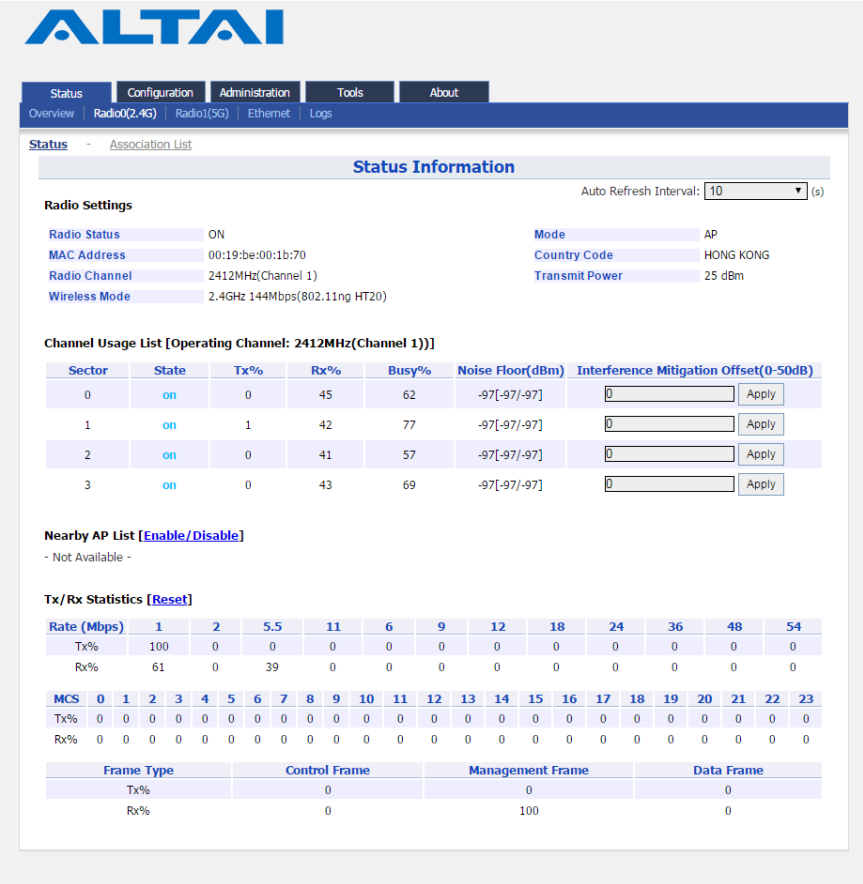


Figure 85 – Radio 0 Status (detail)

Altai Technologies Ltd. All rights reserved

Radio Settings

Radio Status – indicate the current status of Radio 0 interface
MAC – MAC address of Radio 0 interface
Radio Channel - indicate operating frequency (channel) of Radio 0
Wireless Mode – indicate 802.11 standards that Radio 0 operates
Mode – indicate operating mode of Radio 0
Country Code – indicate country code setting of Radio 0
Transmission Power – indicate the total transmission power of Radio 0

Channel Usage List

Tx(%) – average transmit frames percentage of operating channel
Rx(%) – average receive frames percentage of operating channel
Busy (%) – average busy state percentage of operating channel
Noise Floor (dBm) – in ate noise floor of operating channel and noise floor of chain 0, chain 1, and chain 2 on the control channel; if operating with 40MHz bandwidth, it shows the noise floor of chain 0, chain 1, and chain 2 on the extension channel as well.
Interference Mitigation Offset (0-50dB) – signal offset option that will mask all noise / valid signal below *0-50* dB; *0* denotes disabled

Nearby AP List

If Nearby AP List is enabled, device collects nearby AP information and builds Nearby AP List from all beacon frames received during operation. Information shows the SSID, BSSID, authentication mode, cipher mode, operating channel, data rate, and received SNR of collected APs.

Tx/Rx Statistics

This statistic shows traffic distribution about Radio 0 interface. The statistical data includes distribution in terms of data rate and frame type for all incoming and outgoing data frame via Radio 0 interface.

Altai Technologies Ltd. All rights reserved

6.3.2. Status > Radio0(2.4G) > Association List

This information is available on AP mode and Repeater mode only.

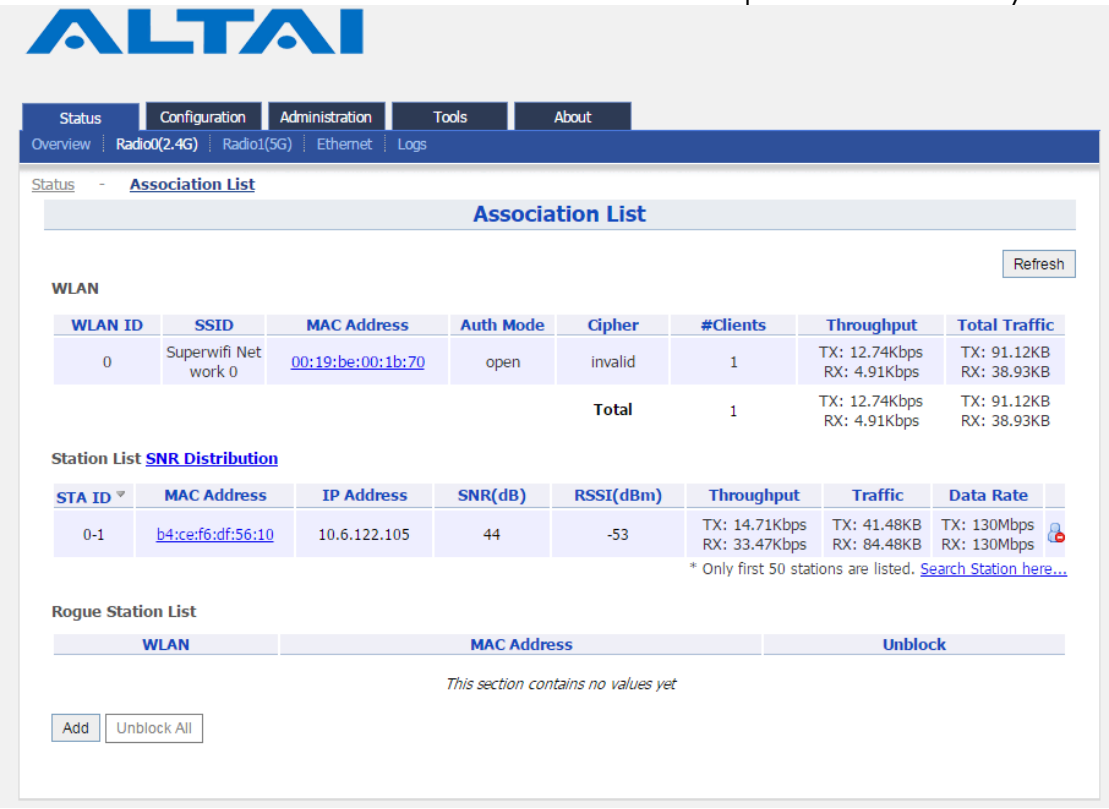


Figure 86 – Radio 0 Association List

WAN

It shows the current status of all operating WLAN on Radio 0 interface. The information includes WLAN ID, SSID, MAC Address, authentication mode, cipher mode, number of associated clients, instant throughput, and total traffic of each operating WLAN respectively.

Station List

It shows the real time status of first 50 associated stations. The status includes Station ID, MAC Address, IP address, SNR(dB) of uplink, RSSI (dBm) of uplink, instant throughput, cumulated traffic of uplink and downlink, and instant data rate of uplink and downlink for each associated station respectively.

Rogue Station List

It lists out the stations that can potentially disrupt wireless networks and can sometimes cause irrevocable damage to the network owners. Network administrator inputs the rogue station's MAC address manually or selects any station from the station List by clicking .

Altai Technologies Ltd. All rights reserved

6.4. Status > Radio1(5G)

6.4.1. Status > Radio1(5G) > Status

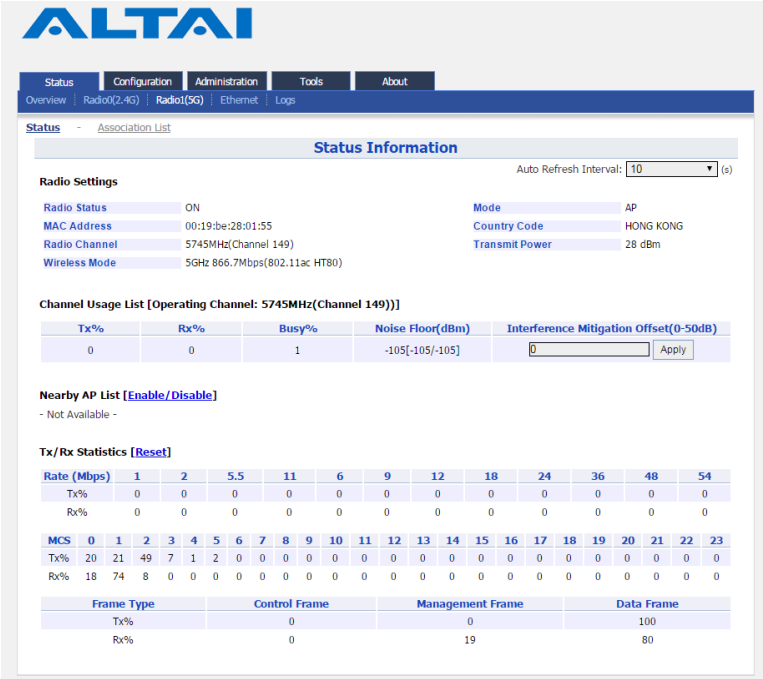


Figure 87 – Radio 1 Status Information

Radio Settings

Radio Status – indicate the current status of Radio 1 interface
MAC – MAC address of Radio 1 interface
Radio Channel - indicate operating frequency (channel) of Radio 1
Wireless Mode – indicate 802.11 standards that Radio 1 operates
Mode – indicate operating mode of Radio 1
Country Code – indicate country code setting of Radio 1
Transmission Power – indicate the total transmission power of Radio 1

Channel Usage List

Tx(%) – average transmit frames percentage of operating channel
Rx(%) – average receive frames percentage of operating channel
Busy (%) – average busy state percentage of operating channel
Noise Floor (dBm) – indicate noise floor of operating channel and noise floor of chain 0, chain 1, and chain 2 on the control channel; if operating with 40MHz bandwidth, it shows the noise floor of chain 0, chain 1, and chain 2 on the extension channel as well.
Interference Mitigation Offset (0-50dB) – signal offset option that will mask all noise / valid signal below *0-50* dB; *0* denotes disabled

Altai Technologies Ltd. All rights reserved

Nearby AP List

If Nearby AP List is enabled, device collects nearby AP information and builds Nearby AP List from all beacon frames received during operation. Information shows the SSID, BSSID, authentication mode, cipher mode, operating channel, data rate, and received SNR of collected APs.

Tx/Rx Statistics

This statistic shows traffic distribution about Radio 1 interface. The statistical data includes distribution in terms of data rate and frame type for all incoming and outgoing data frame via Radio 1 interface.

6.4.2. Status > Radio1(5G) > Association List

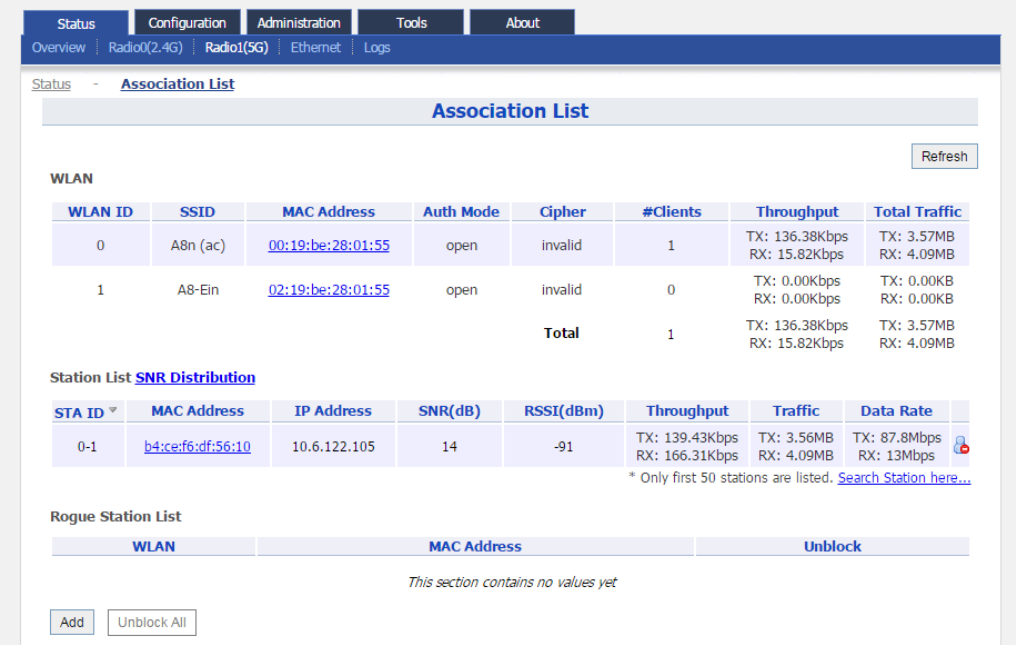


Figure 88 – Radio 1 Association List

WAN

It shows the current status of all operating WLAN on Radio 0 interface. The information includes WLAN ID, SSID, MAC Address, authentication mode, cipher mode, number of associated clients, instant throughput, and total traffic of each operating WLAN respectively.

Station List

It shows the real time status of first 50 associated stations. The status includes Station ID, MAC Address, IP address, SNR(dB) of uplink, RSSI (dBm) of uplink, instant throughput, cumulated traffic of uplink and downlink, and instant data rate of uplink and downlink for each associated station respectively.

Altai Technologies Ltd. All rights reserved

Rogue Station List

It lists out the stations that can potentially disrupt wireless networks and can sometimes cause irrevocable damage to the network owners. Network administrator inputs the rogue station's MAC address manually or selects any station from the station List by clicking  .

Altai Technologies Ltd. All rights reserved

6.5. Status > Ethernet

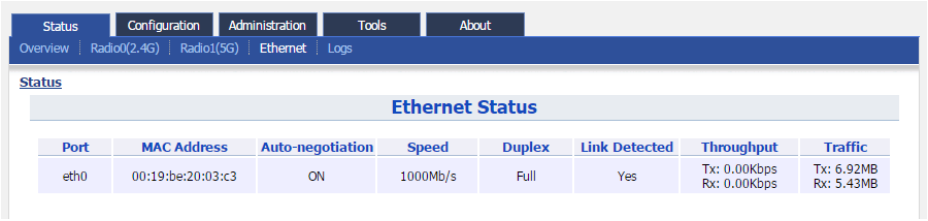


Figure 89 – Ethernet Status (detail)

6.5.1. Status > Ethernet > Status

It shows the current status of Ethernet interfaces. The information includes Port, MAC Address, Auto-negotiation, Speed, Duplex, Link Detected, instant throughput of uplink and downlink and traffic of of uplink and downlink on Ethernet 0 and Ethernet 1 respectively.

6.6. Status > Logs

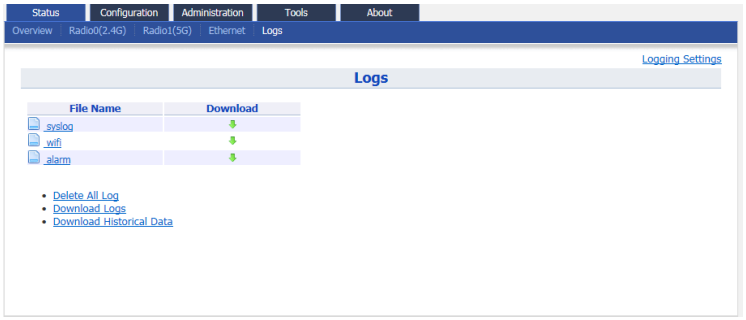


Figure 90 – Status > Logs

In order to realize easier monitoring and diagnosis, A8n (ac) products provide log function for system information, association activity, and alarm event.

syslog – records the information about system information, such as software, hardware, system configuration, and self-checking result

wifi – records the information about association activity, such as association, dissociation, and roaming event

alarm – records the alert information of A8n (ac) device, such as radio down, too high CPU usage

Note:

- Syslog is one of the vital information for Altai's engineer for troubleshooting. It is highly recommended that syslog MUST be enabled

Altai Technologies Ltd. All rights reserved

7. Embedded Tools for Deployment / Operation / Troubleshooting

A8n (ac) products have various tools to help network administrator or engineer on deployment, operating, and troubleshooting. Tools include channel scan, ping … etc.

7.1. Channel Scan

Network administrator and engineer collect the status of 2.4GHz radio and 5GHz radio in the surrounding area. Throughout this tool, network administrator and engineer collect noise floor, percentage of channel busy, and the number of BSS in particular radio channels.

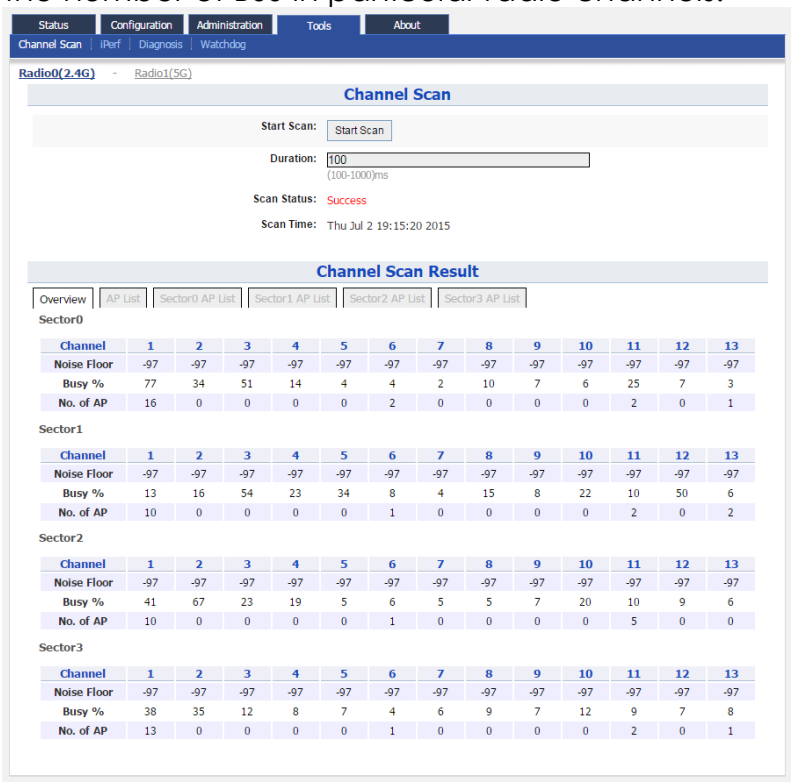


Figure 91 – Chanel Scan Result (Overview)

A8n (ac) shows the channel scan result into Overview tab and AP List tab.

Overview Tab – displays general information from channel 1 to channel 11 at different sector. Information includes noise floor, percentage of channel busy, and the number of BSS on each channel respectively.

AP List Tab - displays information scanned WLAN; information includes SSID, BSSID, authentication Mode, cipher, channel, rate in kbps, and received SNR (dB)

Altai Technologies Ltd. All rights reserved

Sector X AP List Tab– displays information scanned WLAN in sector 0 – 4. X is the sector number. Information includes SSID, BSSID, authentication Mode, cipher, channel, rate in kbps, and received SNR (dB)

7.1.1. Perform channel scan on 2.4G radio

1. Go to **Tools** > **Channel Scan > Radio 0 (2.4G)**
2. [Optional] Provide channel scan interval from 100ms to 1000ms in **Duration**
3. Click **Start Scan**
4. Wait until Scan Status is changed from *In Process* to *Success*; it will take for 20 seconds approximately

Note:
- Wi-Fi service will be interrupted during channel scan

7.1.2. Perform channel scan on 5G radio

1. Go to **Tools** > **Channel Scan** > **Radio 1 (5G)**
2. [Optional] Provide channel scan interval from 100ms to 1000ms in **Duration**
3. Click **Start Scan**
4. Wait until Scan Status is changed from *In Process* to *Success*; it will take for 20 seconds approximately

Note:
- Wi-Fi service will be interrupted during channel scan

7.2. iPerf

A8n (ac) Series products embed iPerf server tool. Network Administrator / Engineer can test the throughput performance via Ethernet, Radio0, or Radio1 with this built-in tool.

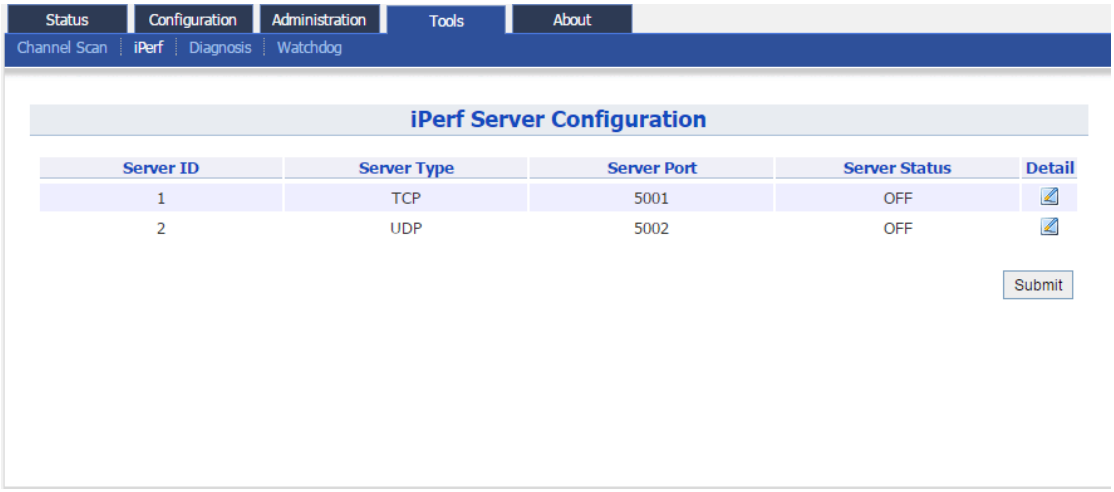


Figure 92 – iPerf Server Configuration

Altai Technologies Ltd. All rights reserved

7.2.1. Enable iPerf TCP Server

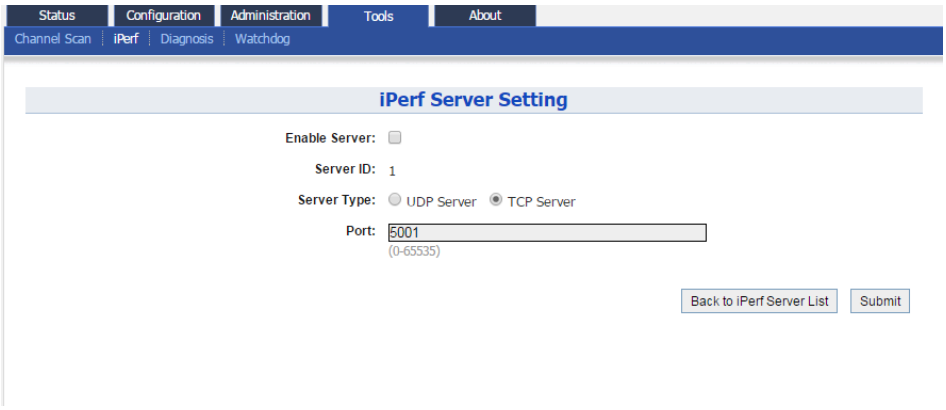


Figure 93 – iPerf TCP Server Setting

1. Go to **Tools** > **iPerf**
2. Click of either **Sever ID 1** or **Sever ID 2**
3. Click **Enable Server** checkbox to enable iPerf TCP Server
4. Click **TCP Server** checkbox
5. Specify the listening port between *0* and *65535* on **Port** [Optional]
6. Click **Submit**
7. Click **Save & Apply**

7.2.2. Enable iPerf UDP Server

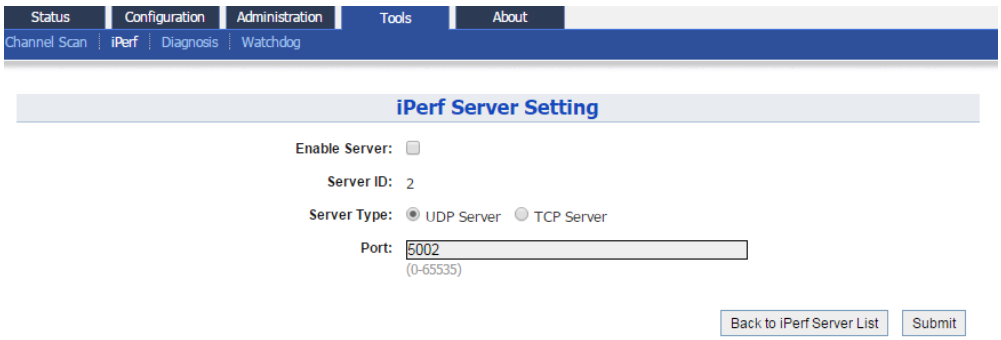


Figure 94 – iPerf UDP Server Setting

1. Go to **Tools** > **iPerf**
2. Click of either **Sever ID 1** or **Sever ID 2**
3. Click **Enable Server** checkbox to enable iPerf UDP Server
4. Click **UDP Server** checkbox
5. Specify the listening port between *0* and *65535* on **Port** [Optional]
6. Click **Submit**
7. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

7.3. Diagnosis

7.3.1. Ping Test

Network administrator and engineer test the reachability of a host and measures the round-trip time between A8n (ac) and the host over an Internet Protocol (IP) network by using ping tool.

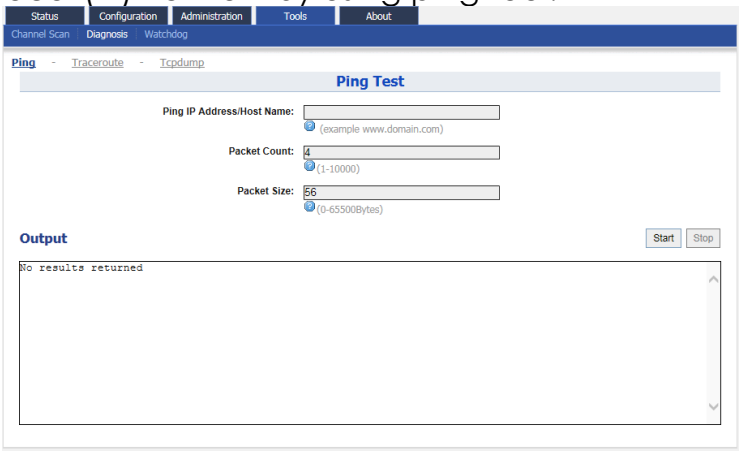


Figure 95 – Ping Test

7.3.2. Perform ping test

1. Go to **Tools** > **Diagnosis** > **Ping**
2. Type target IP address / host name in **Ping IP Address/Host Name**
3. [Optional] Specify how many ICMP (ping) packet that A8n (ac) sends to the target host in **Packet Count**; *4* is default setting
4. [Optional] Specify the packet size of ICMP packet in **Packet Size**; *56* is default setting
5. Click **Start**
6. Click **Stop** to terminate ping test if necessary

7.3.3. Traceroute Test

Network administrator tests the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network by using traceroute test.

Altai Technologies Ltd. All rights reserved

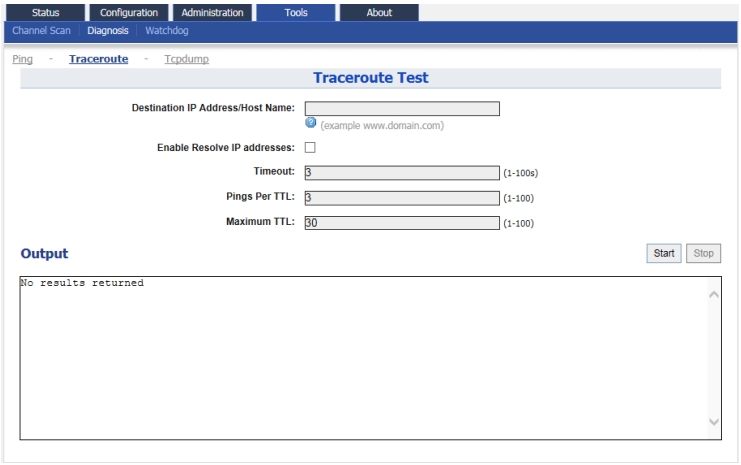


Figure 96 – Traceroute Test

How to perform traceroute test

1. Go to **Tools** > **Diagnosis** > **traceroute**
2. Type target IP address / host name in **Destination IP Address/Host Name**
3. [Optional] Click **Enable Resolve IP addresses** checkbox to enable IP address to domain name translation
4. [Optional] Specify timeout interval between *1*s and *100*s in **Timeout** for traceroute test
5. [Optional] Specify TTL value between *1* and *100* in **Pings Per TTL**; *3* is default setting
6. [Optional] Specify TTL value between *1* and *100* in **Maximum TTL**; *30* is default setting
7. Click **Start**
8. Click **Stop** to terminate ping test if necessary

7.3.4. Tcpdump

A8n (ac) provides a tool to capture packets that passing through a particular interface. It helps network administrator for troubleshooting.

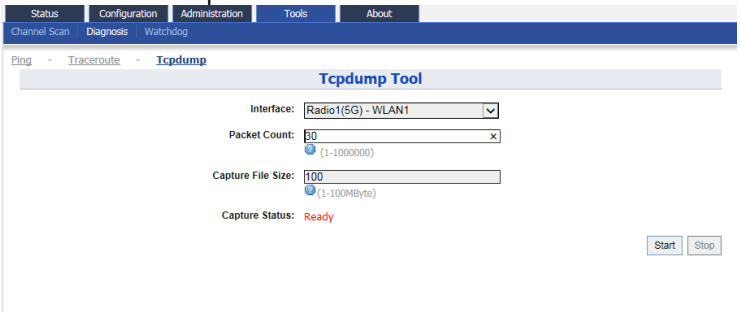


Figure 97 – Tcpdump Tool

How to perform packet capture on A8n (ac)'s interface

1. Go to **Tools** > **Diagnosis** > **Tcpdump**
2. Select suitable interface in **Interface**

Altai Technologies Ltd. All rights reserved

3. [Optional] Specify maximum number of packet in **Packet Count**
4. [Optional] Specify maximum file size in **Capture File Size**
5. Click **Start**
6. Click **Stop** to terminate ping test if necessary
7. Download capture file after finished.

7.4. Watchdog

Watchdog is an electronic timer that is used to detect and recover from system malfunctions. That is timer for periodic reboot.

7.4.1. Schedule Reboot

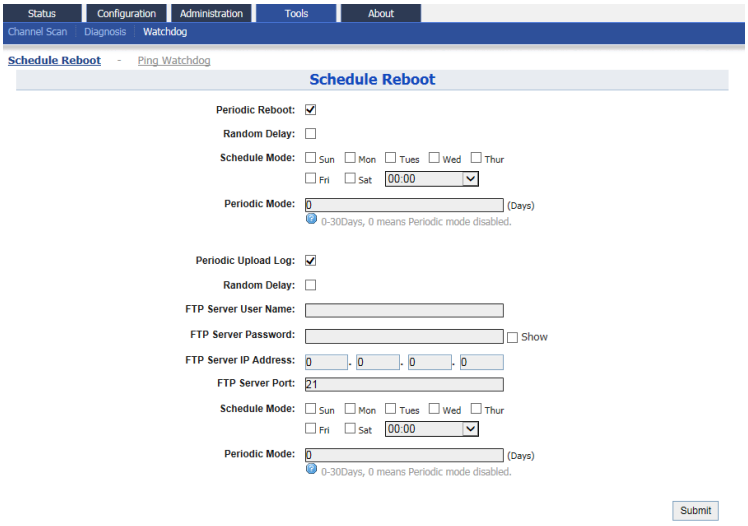


Figure 98 – Schedule Root

Enable periodic reboot

1. Go to **Tools** > **Watchdog** > **Schedule Reboot**
2. Click **Periodic Reboot** to enable reboot scheduler
3. You may change the following settings:
   Radom Delay – Select the checkbox to enable a random delay on scheduled rebooting time. It prevents all APs reboot at the same time
   Schedule Mode Select exact time and day(s) for rebooting device
   Periodic Mode Select a countdown timer (minute) for rebooting device
4. Click **Submit**
5. Click **Save & Apply**

Enable periodic log upload

1. Go to **Tools** > **Watchdog** > **Schedule Reboot**
2. Click **Periodic Upload Log** to enable upload log scheduler
3. You may change the following settings:

Altai Technologies Ltd. All rights reserved

Radom Delay – Select the checkbox to enable a random delay on scheduled rebooting time. It prevents all APs reboot at the same time
FTP Server User Name – Type in username for logging in remote FTP server
FTP Server Password – Type in password for logging in remote FTP server
FTP Server IP Address - Type in IP address of remote FTP server
FTP Server Port - Specify service port of remote FTP server; *21* is default setting
Schedule Mode Select exact time and day(s) for uploading log
Periodic Mode Select a countdown timer (minute) for uploading log

4. Click **Submit**
5. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

7.4.2. Ping Watchdog

Ping watchdog is mechanism that A8n (ac) reboots itself if it fails to communicate (ping) to target host for serval time.

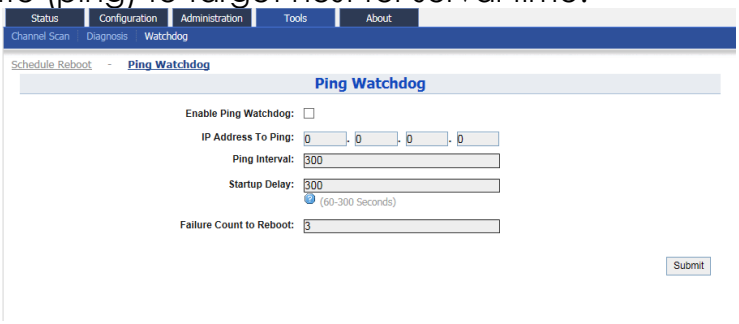


Figure 99 – Ping Watchdog

Enable ping watchdog

1. Go to **Tools** > **Watchdog** > **Ping watchdog**
2. Click **Enable Ping Watchdog** to enable this function
3. Type in IP address of target host in **IP Address To Ping**
4. [Optional] Specify interval between each ICMP request in **Ping Interval**; *300* is default setting
5. [Optional] Specify delay time of each ICMP request in **Startup Delay**; *300* is default setting
6. [Optional] Specify fail tolerant in **Failure Count to Reboot**; *3* is default setting
7. Click **Submit**
8. Click **Save & Apply**

Altai Technologies Ltd. All rights reserved

8. Collect Device's Product Information

A8n (ac) product shows the information about product information, hardware, software and company information in **About** tab.

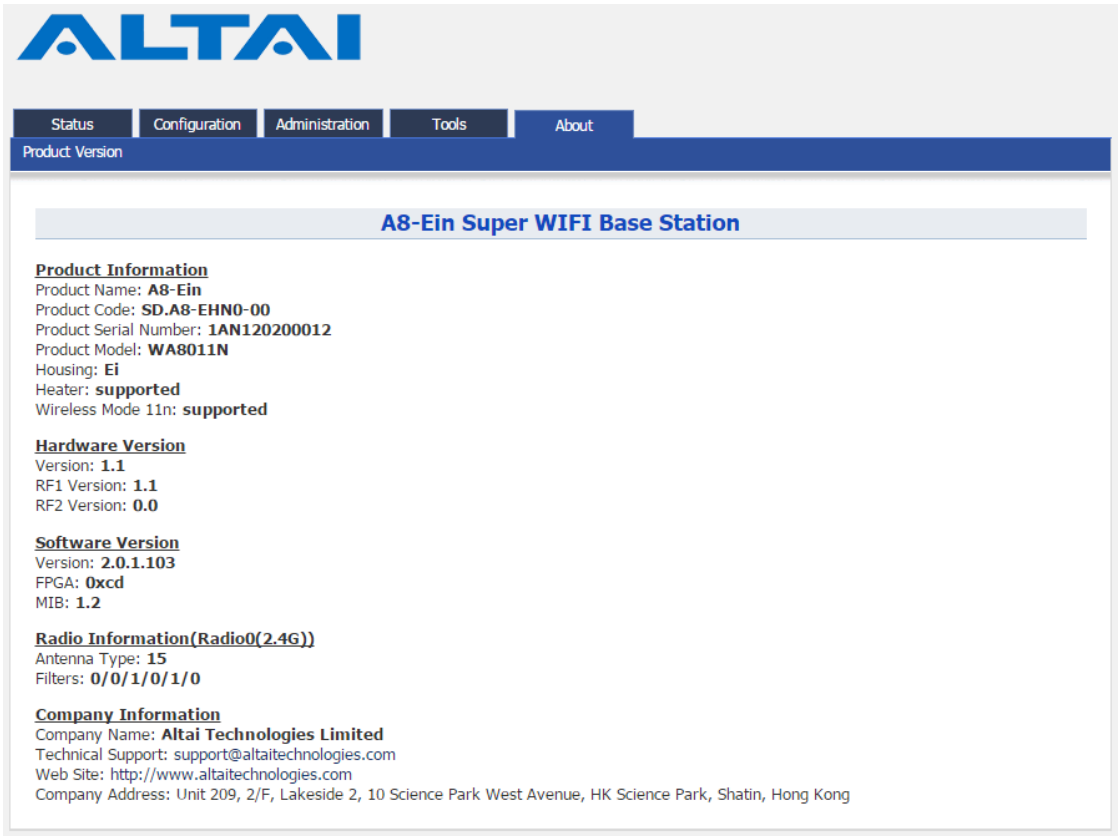


Figure 100 – About tab of A8n (ac) product

Altai Technologies Ltd. All rights reserved