

R1.2.6 Firmware Release note

(Updated to v1.2.6.1701)

Date: Nov, 2015

This release note applies to all products with firmware release v1.2.6.1701.

1. What's New in v1.2.6.1701

1.1. Features and Enhancements

Category	Name	Products Involved
Wireless	ACS channel configuration and algorithm enhancement	A8 series A2 series

2. What's New in v1.2.6.1600

2.1. Features and Enhancements

Category	Name	Products Involved
Operation & Management	Disable guest login via SSH / console	ALL

3. What's New in v1.2.6.1305

3.1. Features and Enhancements

Category	Name	Products Involved
Wireless	Support additional 5G channels (Ch169 and Ch173) for both RoW & India country codes	A8n series A2 series C1an

4. What's New in v1.2.6.1203

4.1. Features and Enhancements

Category	Name	Products Involved
Wireless	Support roaming in station mode	All
	Support Thin AP mode	A2 series C1n series
	Support RADIUS accounting per SSID	All
	Support Dynamic Frequency Selection (DFS) in 5G radio	All
	Support static bridge mode	C1an
	Enhance maximum clients per radio	A2 series C1n series
	Support WPA-Auto and WPA-PSK-Auto authentication	All
	Support web admin login with RADIUS authentication	All
	Support configurable individual sector transmission power	A8n series
	Support Nearby AP list	All
	Support beacon Interval auto tuning	All
	Support SSID locking through brand customization	All
	Support on-the-fly change of Access Control List (ACL) without service disruption	All
	Priority order for AP selection in Station mode, when both Preferred AP List and Roaming Settings are configured	All
	Support MAC address clone in station mode	C1n series
Networking	Support DHCP Option 60	All
	Support SNR LED indication for antenna alignment	A2 series
Operation & Management	Support company address in product information	All
	Log user login event in system log	All
Platform	Support ping watchdog	All

5. Features and Enhancements Descriptions

5.1. ACS channel configuration and algorithm enhancement

From v1.2.6.1701 onwards, A8n and A2 series support configurable channel list for ACS. Users are able to configure any subset of channels for the ACS feature. By default, Ch 1/6/11 is the channel pool for AP selection on 2.4G radio if not specified by the users. As for 5G radio, AP will scan all channels for its selection.

For the best channel selection, A8 and A2 series use total RSSI instead of average RSSI from the received beacons of surrounding APs. For example, CH1 has 3 AP where the RSSI are 10,10,10. CH6 has 1 AP where the RSSI is 15. Old algorithm will pick CH1 because the average RSSI of CH1 is lower. However, CH6 should be more preferable as less AP is using that Channel. In addition, channels with Noise floor > -70dBm are rejected for selection.

5.2. Wireless - Support additional 5G channels (Ch169 and Ch173) for both RoW & India country codes

From v1.2.6.1305 onwards, A8n, A2 and C1an series support the following two additional 5G channels under both RoW and India country codes:

1. Channel 169 (5845MHz)
2. Channel 173 (5865MHz)

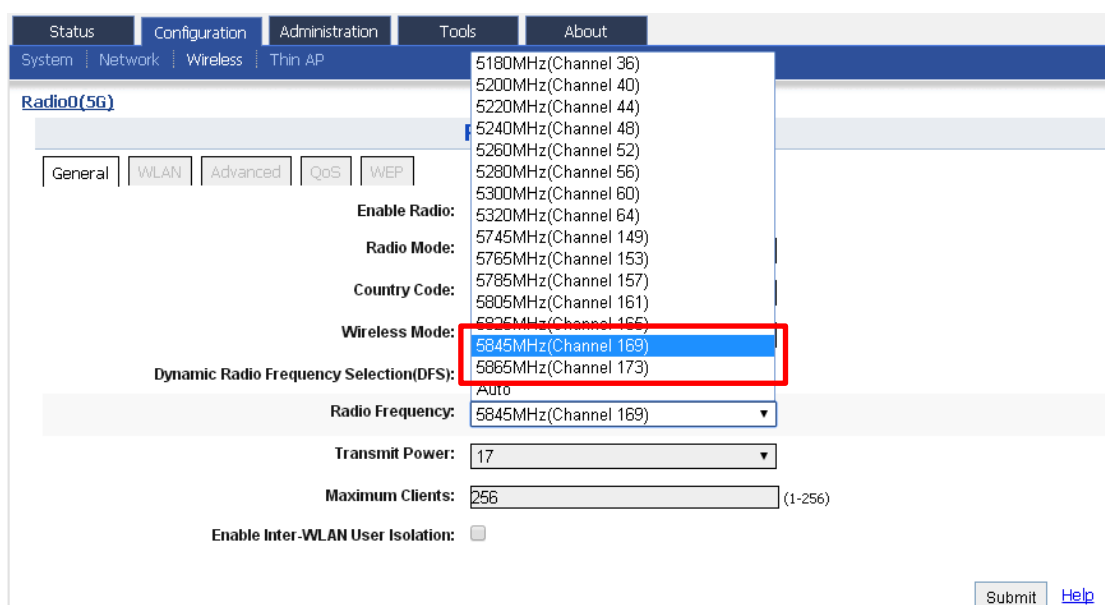


Figure 1 – Additional 5G Channel Support

5.3. Wireless - Support roaming in station mode

From v1.2.6.1203 onwards, all products support roaming in station mode. When enabled, station performs channel scanning and roams to other AP with better SNR based on specified scanning & roaming parameters; otherwise, it never performs channel scanning and associates with the other AP if the current connection is broken.

Roaming Setting

Enable Roaming: ☒

Scan SNR threshold: (0-100dB)

Roaming SNR threshold: (0-100dB)

Max Scan Interval: (1-3600s)

Min Scan Interval: (1-60s)

Scan SNR Fluctuation Threshold: (0-10dB)

Roaming Hysteresis: ☒

Background Scan Channel: ☐ 2412MHz(Channel 1) ☐ 2417MHz(Channel 2) ☐ 2422MHz(Channel 3) ☐ 2427MHz(Channel 4) ☐ 2432MHz(Channel 5)
 Scan all channels if no channel is checked.

[Help](#)

Figure 2 – Roaming Setting

Parameter	Description
Roaming(Enable/Disable, default Disabled)	Enable or disable the roaming feature
Scan SNR Threshold (0-100dB, default 35)	Station performs channel scanning if the SNR of received signal from associated AP is worse than this threshold * Scan SNR Threshold must be larger (>) than Roaming SNR Threshold
Roaming SNR Threshold (0-100dB, default 30)	Station triggers the roaming if the SNR of received signal from associated AP is less than this threshold.
Max Scan Interval (1-3600s, default 60s)	Specify the maximum duration for channel scanning
Min Scan Interval (1-60s, default 10s)	Specify the minimum duration for channel scanning
Scan SNR Fluctuation Threshold (0-10dB, default 5)	If the current AP's signal fluctuation (compared with previous scan result) is higher than the threshold, the

5)	station will do scanning.
Roaming Hysteresis (Enable/Disable, default Enabled)	When enabled, station will be more stickier to current associated AP.
Scan Channel List	Specify the particular channel for scan

Table 1 – Parameters in Roaming Setting

5.4. Wireless - Support Thin AP mode [A2 series and C1n series]

From v1.2.6.1203 onwards, all products in A2 series and C1n series support Thin-AP mode.

Figure 3 – Thin AP configuration

5.5. Wireless - Support RADIUS accounting per SSID

From v1.2.6.1203 onwards, all products support RADIUS Accounting with external RADIUS server. Each SSID could be configured with maximum two RADIUS servers for accounting. IP address of RADIUS accounting server, service port of RADIUS accounting server, and secret must be specified in configuration.

Radio0(2.4G):WLAN0 Setting

WLAN General
WLAN Security
Rogue Station List
QoS
Bandwidth Control

WLAN Security Setting

Authentication Mode: WPA2

Cipher Mode: AES

Group Key Update Interval: 86400 (s)

RADIUS Server Setting

NAS Identifier: (0-32)

RADIUS Server IP Address Type: ☒ IPv4 ☐ IPv6

RADIUS Retry Timeout: 300 (0-65535 s)

	IP Address	Port	Secret(1-128)	
RADIUS Server	0 . 0 . 0 . 0	1812		Show
Secondary RADIUS Server	0 . 0 . 0 . 0	1812		Show

RADIUS Accounting Server Setting

RADIUS Accounting Server IP Address Type: ☒ IPv4 ☐ IPv6

Accounting Interim Interval: 300 (60-86400s, 0:Disable)

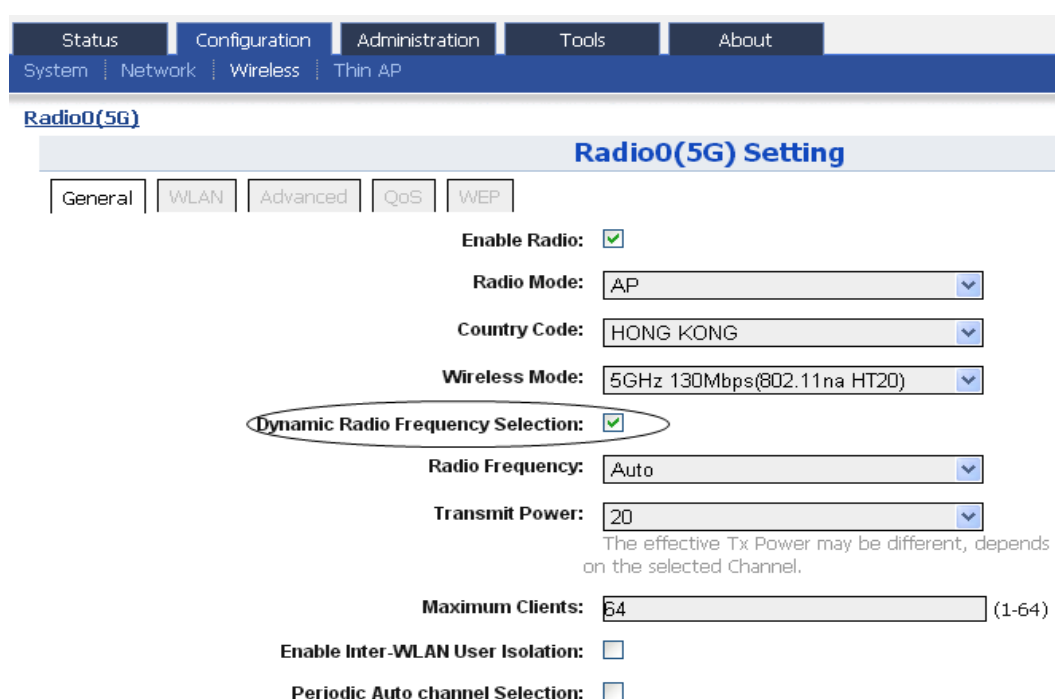
	IP Address	Port	Secret(1-128)	
RADIUS Accounting Server	0 . 0 . 0 . 0	1813		Show
Secondary RADIUS Accounting Server	0 . 0 . 0 . 0	1813		Show

Figure 4 – RADIUS accounting setting

5.6. Wireless - Support Dynamic Frequency Selection (DFS) in 5G radio

From v1.2.6.1203 onwards, all products support Dynamic Frequency Selection (DFS) in their 5G radio. DFS is a mechanism to allow unlicensed devices to use the 5 GHz frequency bands already allocated to radar systems without causing interference to those radars. When enabled, AP monitors radar during CAC period. Provided that no radar is detected during CAC period, a communication link is established on the selected channel. CAC period is 10 minutes between 5.6GHz and 5.65GHz; while CAC period is 60 seconds outside 5.6GHz and 5.65GHz.

Remark: The Radio Frequency must be set to "Auto".



The screenshot shows the configuration interface for the Altai Super WiFi. The top navigation bar includes 'Status', 'Configuration', 'Administration', 'Tools', and 'About'. Below this, a sub-navigation bar shows 'System', 'Network', 'Wireless', and 'Thin AP'. The main content area is titled 'Radio0(5G)' and 'Radio0(5G) Setting'. It features several tabs: 'General', 'WLAN', 'Advanced', 'QoS', and 'WEP'. The 'General' tab is selected, showing the following settings:

- Enable Radio:** ☒
- Radio Mode:** AP (dropdown)
- Country Code:** HONG KONG (dropdown)
- Wireless Mode:** 5GHz 130Mbps(802.11na HT20) (dropdown)
- Dynamic Radio Frequency Selection:** ☒ (This checkbox is circled in red in the original image)
- Radio Frequency:** Auto (dropdown)
- Transmit Power:** 20 (dropdown)
- The effective Tx Power may be different, depends on the selected Channel.
- Maximum Clients:** 64 (1-64)
- Enable Inter-WLAN User Isolation:** ☐
- Periodic Auto channel Selection:** ☐

Figure 5 - Dynamic Frequency Selection

5.7. Wireless - Support static bridge mode [C1an]

From v1.2.6.1203 onwards, C1an supports bridge mode.

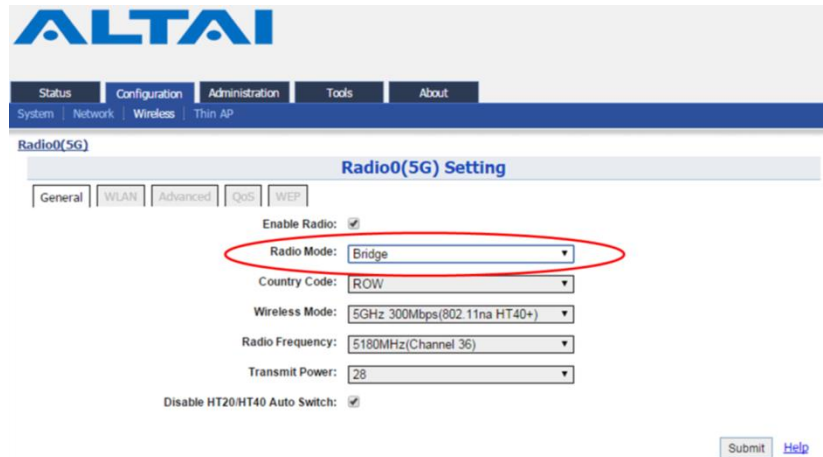


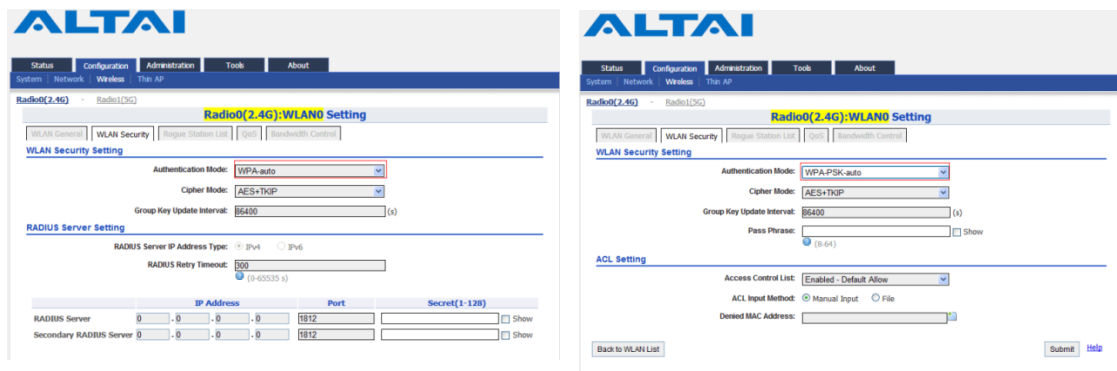
Figure 6 – Bridge mode in C1an

5.8. Wireless - Enhance maximum clients per radio [A2 series and C1n series]

From v1.2.6.1203 onwards, all products of A2 series and C1n series support maximum 256 clients per radio.

5.9. Wireless - Support WPA-Auto and WPA-PSK-Auto authentication

From v1.2.6.1203 onwards, all products support both WPA-Auto and WPA-PSK-Auto authentication. If AP is configured with WPA-Auto authentication, it supports clients using either WPA or WPA2 authentication; while AP supports clients using either WPA-PSK or WPA2-PSK authentication if it is configured with WPA-PSK-Auto authentication.



(a)

(b)

Figure 7 – WLAN authentication setting – (a) WPA-Auto, (b) WPA-PSK-Auto

5.10. Wireless - Support web admin login with RADIUS authentication

From v1.2.6.1203 onwards, all products support three authentication options (Local/RADIUS/RADIUS + Local) for logging in web GUI. A maximum of two RADIUS servers (one for backup) are supported for login authentication.

The screenshot shows the ALTAI web interface. At the top is the ALTAI logo. Below it is a navigation bar with tabs: Status, Configuration, Administration, Tools, and About. Under 'Administration', there are links: User Admin, Web Admin, SNMP, Certificate, Firmware Update, Factory Default, Backup / Restore, Customization, and License. The 'User Admin' section is active, showing a login form with fields for Username (set to 'admin'), Password, and Confirm Password, and a Submit button. Below this is the 'Login Authentication Setting' section, which contains a dropdown menu for 'Authentication Type'. The dropdown is open, showing four options: 'RADIUS Authentication', 'Local Authentication', 'RADIUS Authentication' (which is highlighted), and 'RADIUS+Local Authentication'. A Submit button is located to the right of the dropdown.

Figure 8 – Login Authentication Setting

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 2 – Different authentication type

5.11. Wireless - Support configurable individual sector transmission power [A8n series]

From v1.2.6.1203 onwards, A8n series support transmission power configuration on each individual sector in their 2.4G radio.

Enable Radio: ☒

Radio Mode: AP

Country Code: HONG KONG

Wireless Mode: 2.4GHz 130Mbps(802.11ng HT20)

Radio Frequency: 2452MHz(Channel 9)

Transmit Power: 27

Maximum Clients: 512 (1-512)

Enable Inter-WLAN User Isolation: ☐

Range Optimization: Auto

Sector Power Control: ☒

Sector	State	Sector Power
0	☒ On ☐ Off	27
1	☐ On ☐ Off	27
2	☐ On ☐ Off	27
3	☐ On ☐ Off	27

Figure 9 –Transmission Power Setting of Individual Antenna Sector

5.12. Wireless - Support Nearby AP list

From v1.2.6.1203 onwards, all products support sniffing function on both 2.4G radio and 5G radio. When Sniffing is enabled, AP collects nearby AP information and builds Nearby AP List from all beacon frames received during operation. The Nearby AP List supports at least 128 entries including AP with hidden SSID.

Channel Usage [Operating Channel: 2412MHz(Channel 1)]

Tx% (Avg)	Rx% (Avg)	Busy% (Avg)	Noise Floor(dBm)	CTL0	CTL1	EXT0	EXT1	Interference Mitigation Offset(0-50dB)
3%(0%)	42%(44%)	63%(66%)	-97	-97	-95	0	0	0

Nearby AP List [Enable/Disable]

SSID	BSSID	Auth Mode	Cipher	Channel	Rate(Kbps)	SNR(dB)
altai_backhaul_24g	22:19:be:80:fa:5a	wpa2-psk	aes	1	130000	31
Superwifi Network 1	02:19:be:80:b3:51	open	none	1	130000	33
altai_network_x	00:19:be:80:fa:5a	wpa	aes	1	130000	31
altai_network_wpa	02:19:be:80:fa:5a	wpa2-psk	aes	1	130000	31
Superwifi Network 3	22:19:be:80:b3:51	open	none	1	130000	33
altai_guest	12:19:be:80:fa:5a	open/shared	wep	1	130000	31
Superwifi Network 0	00:19:be:80:b3:51	open	none	1	130000	32
TP-LINK_2.4GHz_5A4C57	64:66:b3:5a:4c:57	wpa2-psk	aes	2	450000	9
Charles3	12:19:be:30:72:12	open	none	2	65000	15
CRM23	28:34:a2:7f:54:30	wpa2-psk	aes	2	144400	14

Note:
Information is collected at operating channel only (no scanning on other channels).
SNR of APs from adjacent channels reflects the leaked signal observed at operating channel.

Figure 10 – Nearby AP List

5.13. Wireless - Support beacon Interval auto tuning

From v1.2.6.1203 onwards, all products support auto tuning of the beacon interval, in order to reduce the beacon frame overhead in the wireless network.

Advanced Setting

AMPDU: ☒

AMPDU Limit: (1-64)

AMSDU: ☒

Max Tx Streams:

Max Rx Streams:

Beacon Interval Auto: ☒

Beacon Interval: (40-3500)

Data Rate Setting

Data Rate: (Mbps)

Data Rate Setting:

1Mbps: ☒ Enable ☐ Disable

2Mbps: ☒ Enable ☐ Disable

5.5Mbps: ☒ Enable ☐ Disable

11Mbps: ☒ Enable ☐ Disable

6Mbps: ☒ Enable ☐ Disable

9Mbps: ☒ Enable ☐ Disable

Figure 11 – Beacon interval auto tuning option

5.14. Wireless - Support SSID locking through brand customization

From v1.2.6.1203 onwards, all products support restricting user from modifying SSID configurations. It is enabled through brand customization.

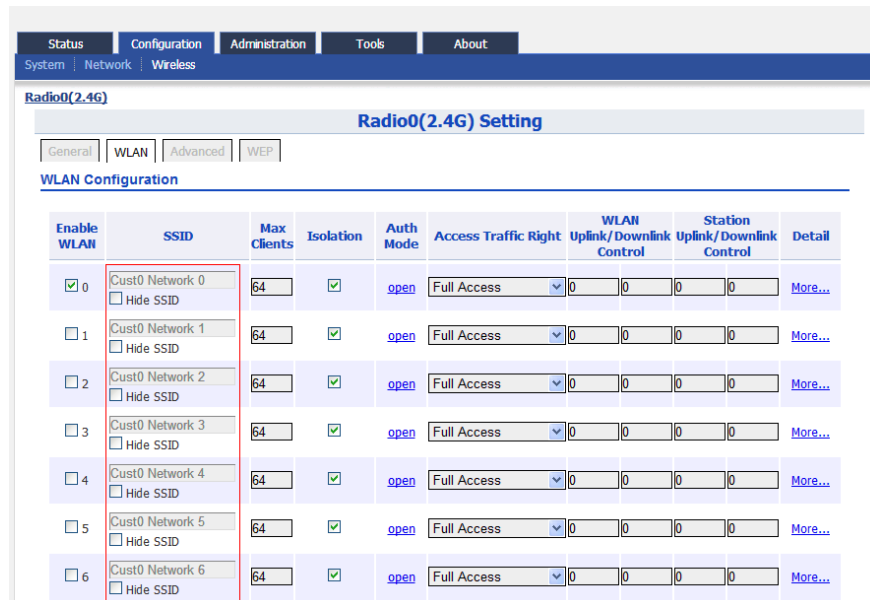


Figure 12 – SSID configuration is restricted when SSID lock is enabled

5.15. Wireless - Support on-the-fly change of Access Control List (ACL) without service interruption

From v1.2.6.1203 onwards, all products support on-the-fly change of ACL in SSID without causing Wi-Fi service interruption.

5.16. Wireless – Priority order for AP selection in Station mode, when both Preferred AP List and Roaming Settings are configured

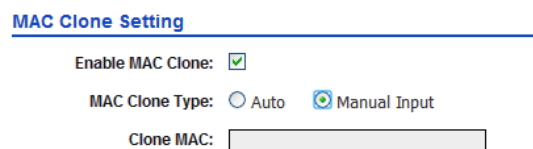
From v1.2.6.1203 onwards, all products in station mode follow the following priority orders when both preferred AP list and roaming setting are configured:

1. When the AP's SNR in preferred AP list is larger than or equal to ($\geq$) roaming SNR threshold, station associates the AP with preferred AP list setting.
2. When the received SNR from AP which is not in preferred AP list is larger than ($>$) roaming SNR threshold, station associates the AP based on received SNR

- When the AP's SNR (no matter in preferred AP list or not) is less than (<) roaming SNR threshold, station associates the AP based on received SNR

5.17. Wireless - Support MAC address clone in station mode [C1n series]

From v1.2.6.1203 onwards, C1n series support MAC address clone in station mode. MAC address could be either input manually or cloned from connection laptop/PC directly. This feature supports one laptop/PC only.



MAC Clone Setting

Enable MAC Clone: ☒

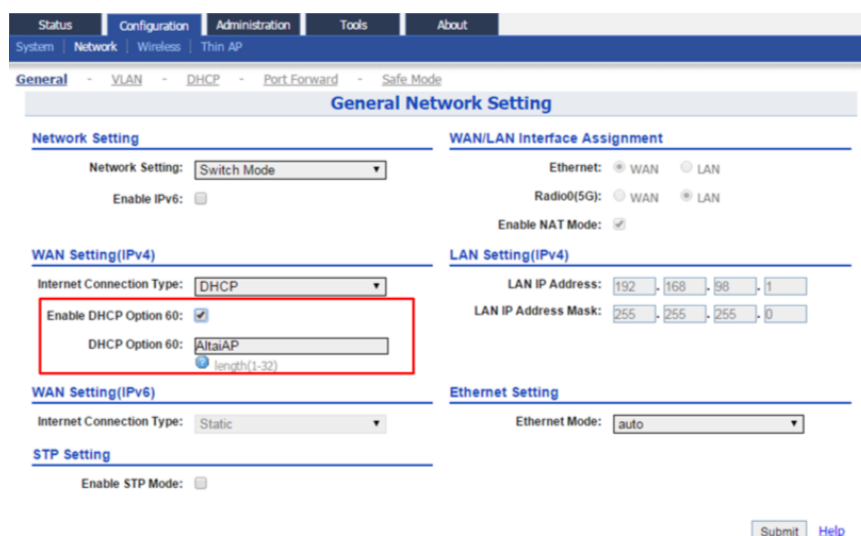
MAC Clone Type: ☐ Auto ☒ Manual Input

Clone MAC:

Figure 13 – MAC Clone Setting

5.18. Networking - Support DHCP Option 60

From v1.2.6.1203 onwards, all products support DHCP option 60. When AP enables DHCP client, it supports DHCP Option 60 in both IPv4 and IPv6. Administrator specifies a string up to 32 characters.



General Network Setting

Network Setting

Network Setting:

Enable IPv6: ☐

WAN Setting(IPv4)

Internet Connection Type:

Enable DHCP Option 60: ☒

DHCP Option 60: length(1-32)

WAN Setting(IPv6)

Internet Connection Type:

STP Setting

Enable STP Mode: ☐

WAN/LAN Interface Assignment

Ethernet: ☒ WAN ☐ LAN

Radio0(5G): ☐ WAN ☒ LAN

Enable NAT Mode: ☒

LAN Setting(IPv4)

LAN IP Address:

LAN IP Address Mask:

Ethernet Setting

Ethernet Mode:

[Submit](#) [Help](#)

Figure 14 – DHCP Option 60

5.19. Networking - Support SNR LED indication for antenna alignment [A2 series]

From v1.2.6.1203 onwards, A2 series support LED indication for aligning the antenna in station mode, repeater mode, and bridge mode. When enabled, administrator specifies the three-level SNR thresholds (Low/Medium/High).



Figure 15 - LED indication for aligning the antenna

The Ethernet LED of device behaves as the followings:

SNR Level	LED behavior
< Low SNR Threshold	LED always OFF
Between Low SNR Threshold and Medium SNR Threshold	LED blinks slowly
Between Medium SNR Threshold and High SNR Threshold	LED blinks quickly
> High SNR Threshold	LED always ON

5.20. Operation & Management - Support company address in product information

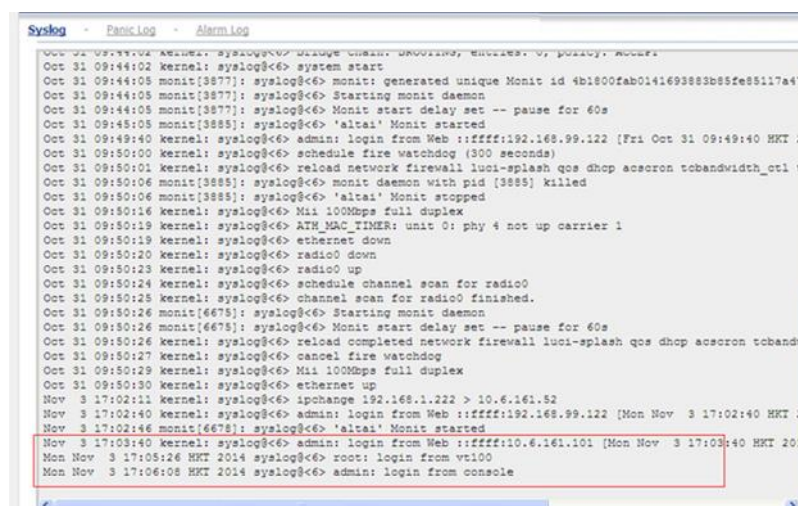
From v1.2.6.1203 onwards, all products have company address in About page. This attribute can be specified through brand customization.



Figure 16 – Company address in about page

5.21. Operation & Management - Log user login event in system log

From v1.2.6.1203 onwards, all products log the user login event via Web/Console/SSH in syslog. The information includes login interface and the user name.



5.22. Platform - Support ping watchdog

From v1.2.6.1203 onwards, all products support ping watchdog. This feature allows devices to ping the target host periodically. The default ping interval (time between ICMP echo requests are sent) is 300 seconds. Startup Delay specifies the initial time delay (in seconds) until the first ICMP echo requests are sent by Ping Watchdog. The default value is 300 seconds. 60 seconds is recommended value for the Startup Delay as the network interface and wireless connection initialization takes a considerable amount of time if the device is rebooted. Failure Count to Reboot Specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, Ping Watchdog will reboot the device. The default value is 3.

ALTAI

Status Configuration Administration Tools About

Channel Scan Diagnose Watchdog

Schedule Reboot - Ping Watchdog

Ping Watchdog

Enable Ping Watchdog: ☐

IP Address To Ping: 0 . 0 . 0 . 0

Ping Interval: 300

Startup Delay: 300 (60-300 Seconds)

Failure Count to Reboot: 3

Submit

Figure 17 – Ping watchdog

6. Bugs Fixed

6.1. *Firmware v1.2.6.1701*

- Improvement of algorithm on AP selection when running in Station mode

6.2. *Firmware v1.2.6.1600*

- Dropbear prints login password to /var/log/messages in plaintext
- Client Drop under High-Concurrent-User / High-Channel-Usage Environment
- System auto reboots frequently under heavy multicast traffic
- High ping loss for clients on sector 0/2/3 (non-master radio sector) of A8n
- WPA-PSK/WPA2-PSK passphrase with space characters at the head and/or tail causes station unable to associate with the VAP

6.3. *Firmware v1.2.6.1305*

- Potential looping issue under thin AP mode with AC central authentication
- DSCP does not prioritize VOIP packet under AP --- Station setup
- Associated client cannot scan other SSIDs in the same AP
- Re-configuration of DSCP values on 5G radio of A2 series products does not take effect
- DSCP mapping would be reset after channel update
- Anomaly of Association Client Status under AP --- Station setup with different security settings
- Reset button does not reset root password

6.4. *Firmware v1.2.6.1203*

- A2 is inaccessible after downgrading with firmware 1.2.3.x
- Options of wireless configuration page are not displayed on Web UI due to insufficient memory
- Web UI responses slowly with heavy traffic on C1n series and A2 series
- C1n (32MB) run unstable due to high memory usage
- Enabling Spanning Tree Protocol (STP) blocks the communication between Wi-Fi clients at both ends with VLAN enabled under back-to-back approach.
- High CPU usage due to handling too many web session concurrently on C1n series and A2 series
- Wi-Fi clients cannot access web UI of A2 in Thin AP mode with access controller under centralized forwarding
- Access controller cannot provision WLAN configuration to A2
- Web UI is inaccessible on remote AP through local AP in bridge mode connection
- User cannot login web UI on A2 via either Firefox or Chrome if the system name of AP contains "&" character
- The setting of Intra-WLAN isolation and Inter-WLAN isolation are not consistence between Web UI and AP system. E.g. Web UI displays Inter-WLAN isolation as disabled If AP is enabled the Inter-WLAN isolation, and vice versa
- DHCP client behind CPE (station mode) cannot renew the IP address after the wireless link is re-established
- C1an does not show the mac clone feature on Web UI in station mode
- Fix Heartbleed Vulnerability from SSH / HTTPS connection

7. Open Issues

- HTTP Error 413 appears if uploading invalid file via firmware update page to AP
- The status of bridge connection might show "Disconnect" on A2 web UI if a bridge link is setup between C1n and A2 successfully
- Warning message "Please use Firefox, Google, IE8+ browser to access the web page, to ensure the best user experience" is missed when accessing web UI with Internet Explorer 7
- Web UI responses slowly or displays error if the Ethernet mode of AP is configured as manual mode and Ethernet Duplex is configured any full duplex mode, e.g. 100Mbps_Full.
- Hidden SSID cannot be scanned in Nearby AP feature
- IP address and SNR of associated C1n (station mode plus gateway mode) are displayed as 0.0.0.0 and 0 on A8n association list respectively
- Incorrect system time and throughput in throughput graph of historical statistic on all products
- Inconsistence frequency channel options on radio interface between AP and access controller