# Firmware for AWK-1131A Series Release Notes

<table>
<thead>
<tr>
<th>Version:  v1.21</th>
<th>Build:  20061018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date:</td>
<td>Jun 30, 2020</td>
</tr>
</tbody>
</table>

## Applicable Products
AWK-1131A series

## Supported Operating Systems
N/A

## New Features
- Added 8 channels (total 11) for Client-based Turbo Roaming channel scanning.
- Added support for Wi-Fi Remote Connection Check.
- Added Indoor/outdoor channel list option.
- Added a progress bar to show the progress of firmware upgrades.
- Added an option to lock a user account when entering an invalid password.
- The system will record a system log if the device IP is changed via the Wireless Search Utility.
- Added support for Yahoo and Google email servers.
- Email messages now include device information.
- Added a function to gather additional Wi-Fi related information.
- Added an option to allow the use of special characters.
- Added support for Remote Diagnostics for engineer support.
- Added an option to show the PSK password in clear text.

## Enhancements
- [WLAN] When in Client Mode, the AWK now take less time to reconnect after being disconnected by the AP.
- [WLAN] When in Client Mode, the AWK now take less time to reconnect if MAC Clone is enabled.
- [WLAN] When in Client Mode, the AWK now take less time to reconnect if the second EAPOL packet is lost.
- [WLAN] When in Client Mode, the AWK now take less time to reconnect when plugging in Ethernet when the WLAN is establishing a connection.

## Bugs Fixed
- [WLAN] The AP responds to unicast probe requests, even if the AP is not the receiver.
- [WLAN] The GARP reply sent by the AP/Client does not have a VLAN tag.
- [WLAN] Unable to establish a Wi-Fi connection with APs that support 802.11r.
- [WLAN] G-mode-only clients are unable to associate with the AP.
- [WLAN] Authentication may fail when the client’s security is set to Enterprise mode.
- [WLAN] The BSS node is cleaned in Master mode.
- [Security] The Wireless Search Utility cannot find clients that use the 4th WEP key.
- [Roaming] The AWK does not connect to the AP with the strongest signal when there is no AP that satisfies the RSSI > keep alive threshold.
- [WEB] Revised the filename of the captured Wi-Fi packets.
- [WEB] CVE-2018-10690: HTTP is enabled and HTTPS is disabled by default.
- [WEB] CVE-2018-10692: The session cookie does not have an HttpOnly flag.
- [WEB] CVE-2018-10695: The send email to admin account function can be used to execute Linux commands on the device.
- [WEB] Specifying the max byte size of the primary RADIUS shared key will change the setting of the secondary RADIUS server IP.
• [WEB] Unable to set VAP3 to VAP9 as the RF-type for A/N Mixed mode, Channel 36, and channel width 20/40 MHz.
• [WEB] The interface shows incorrect channel information.
• [WEB] Wi-Fi channel selection does not work during Quick Setup.
• [WEB] The web server crashes when reading invalid content.
• [DHCP] The number of DHCP server users cannot be set to more than 128.
• [DHCP] The DHCP server does not work properly when AeroMag AP enabled.
• [Configuration] If only the primary RADIUS has been configured, the group check would check the settings of the secondary RADIUS setting.
• [Configuration] When in non-AP mode, when checking channel width 20/40 MHz, the AWK would check channel 165 which does not support 40 MHz.
• [Configuration] Unable to import configuration files after changing the device IP.
• [MAC Clone] The client is unable to restore its original MAC address when unplugged from the LAN after disconnecting from the AP.
• [Mirror Port] Incorrect filename for the mirror port file.
• [LAN] Unable to get the correct speed and duplex mode.
• [Firewall] IP filter does not drop packets if MAC filtering is disabled.
• [Firewall] Ports of device services such as the DHCP server are added to the white list automatically when port filtering is enabled.
• [SNMP] SNMPv3 is unreachable after rebooting.
• [SNMP] SNMP would sometimes cause a memory leak.
• [SNMP] The MIB file name contains an invalid character (_).
• [System Log] The system log does save a configuration change log if the IP is changed via the Wireless Search Utility.
• [MXview] Unable to import or export configuration files and upgrade firmware using MXview.

Changes

• [WLAN] Changed the default multicast rate value.
• [WLAN] Changed the fix rate list according to the selected RF type.
• [WLAN] Changed the management frame rate according to the selected RF type.
• [WLAN] Changed the number of management frame transmission retries from 8 to 4.
• [WLAN] Changed the basic rate of G-only mode to be same rate as 802.11b.
• [Firewall] Increased MAC/IP/Port filter entries up to 60.
• [Firewall] Changed the default rule policy to ACCEPT.
• [WEB] Changed the default system description to the model name.
• [WEB] Changed the web configuration import buffer size from 64K to 128K.
• [Account Status] User-level accounts can now no longer see other user account information.
• [LED] Adjusted the Wi-Fi signal level LED.

Notes
N/A
<table>
<thead>
<tr>
<th>Version: v1.19</th>
<th>Build: Build_18121212</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: Dec 28, 2018</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- IEC 62443-4-2 support
- 3rd SNMP trap server
- Web certificate support

**Enhancements**
N/A

**Bugs Fixed**
- Abnormal roaming handoff time if MAC clone is enabled
- Device reboot if it receives an abnormal beacon which does not follow IEEE standard.
- Issue with the error handler for abnormal Wi-Fi packets

**Changes**
N/A

**Notes**
N/A
<table>
<thead>
<tr>
<th>Version: v1.18</th>
<th>Build: Build_18100315</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: Oct 30, 2018</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
N/A

**Enhancements**
N/A

**Bugs Fixed**
- Abnormal behavior of the DFS function.

**Changes**
N/A

**Notes**
N/A
**Supported Operating Systems**
N/A

**New Features**
- Quick Setup wizard.
- Wi-Fi certificate function.
- Static MAC clone function.
- Wi-Fi Mirror port.
- Management Frame Encryption.
- Tool for setting up Cybersecurity IEC 62443-4-2 Level 1.
- DHCP option 12 (hostname = device name).
- DHCP option 50 (requested IP address).
- Locate Device function.

**Enhancements**
- Supports WLAN system log version 2.
- Supports bridge status via SNMP.
- System log will now have SNMP information if users save configuration settings via SNMP.
- Devices will record a system log entry if an invalid configuration setting is reset to the default value.
- Bridge interface has the ability to forward broadcast ARP reply.
- A new roaming configuration has been created to replace the current configuration to enhance RX accuracy.
- Improved Tx/Rx accuracy.
- A system log file can now record up to 3000 entries.

**Bugs Fixed**
- WLAN Tx/Rx is stuck.
- An AP always works on 20 MHz if there is another AP on the channel when it is booting up.
- Tx hang caused by interrupt (0x0000 0000) messages.
- Facility and severity values in the RSSI report are incorrect.
- Traffic can't pass if the WEP key index is 1.
- DUT reboot if client roams multiple times.
- WLAN is unstable if LFPT and MAC clone are enabled at the same time.
- Configuration import fails if there is a space between an item and its value in the configuration import file.
- SNMP can't get the value of "entryIndex" from the "BridgeStatusEntry" table.
- AP broadcast button can't be enabled/disabled.
- Configuration Import & Export issue in the web console if the encryption method is used to import configuration via ABC-01.
- RSSI report doesn't report the node that is not updated for 1 sec.
- Cannot change the bandwidth to 20/40 MHz in client mode in some cases.
- Roaming log has wrong SNR when the roaming is caused by low signal strength.
- Unexpected roaming occurs because AP Alive check timer resumes after AP receives packets on a foreign channel.
- System log file cannot be exported in Firefox 59.0.2.
- Channel survey table on the Wi-Fi Settings page of Quick Setup shows incorrect information if a
device is running in client mode.
- WLAN connected time is always "0" on MXview & SNMP.
- AP with multiple VAPs only works at 20 MHz even though its bandwidth is configured as 20/40 MHz.
- Login message should use the activated configuration.
- AP alive check does not work in some cases.
- WLAN assoc rx/tx pkts/bytes is always 2147483647 for a value > 2147483647.
- The wireless disable function does not work.
- Cannot configure messages with 240 characters for web login and login authentication failure messages.
- The length of the WEP key 4 does not correspond to the key type and key length in Wi-Fi security of quick setup.
- Network information on the Overview page does not match with the asqc page.
- DHCP client list information can be set via SNMP.
- User can execute Linux commands by entering their username or password in the login window.
- Cannot reboot device through MXconfig.
- Show an error message if the RF type 2.4G N mode (G/N, B/G/N, N only) is selected on the Advanced WLAN Settings page.
- User can’t increase the minimum length setting for passwords if the current password is less than a certain length.
- An User-level user can’t use the Diagnostics and Wi-Fi Mirror Port functions.
- User-level user can’t export current device information on the Troubleshooting page.
- Network information is not current IP/netmask/Gateway when AWK acts as the DHCP client.

Changes
- Initial network IP is set to 169.254.0.1 before an IP address is assigned by the DHCP server for the first time.
- Changed the max length allowed for user passwords from 16 to 32.
- Changed the default value of device name to Model name_xx:yy:zz, xx:yy (zz is the last 3 bytes of the device MAC).
- Changed AP’s inactive timeout range to 8 to 240 sec.
- Changed the range for roaming threshold and AP candidate threshold from 5-40 to 5 -60.
- Changed the UI field name "Signal Strength" to "Signal Level" on the wireless status page.
- Added a "skip" option on the login page where the user is asked to modify the password.
- Applied uniform style to the email, syslog, system, trap server, time setting, and wireless certification pages.
- All buttons on the System Log page are disabled when the log entries are cleared.
Notes
N/A
<table>
<thead>
<tr>
<th>Version: v1.16</th>
<th>Build: Build_17102617</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
N/A

**Enhancements**
N/A

**Bugs Fixed**
- The following CVE's are fixed: CVE-2017-13077, CVE-2017-13078, and CVE-2017-13080

**Changes**
N/A

**Notes**
N/A
### Applicable Products

### Supported Operating Systems
N/A

### New Features
N/A

### Enhancements
- Enhanced the interoperability with APs from other vendors by adjusting the QoS TID behavior.

### Bugs Fixed
- Kernel panic issue when DFS is triggered.

### Changes
N/A

### Notes
- This version includes the changes from firmware v1.12 and v1.13.
Applicable Products

Supported Operating Systems
N/A

New Features
N/A

Enhancements
• Enhanced the interoperability with APs from other vendors by adjusting the QoS TID behavior.

Bugs Fixed
• Kernel panic issue when DFS is triggered.

Changes
N/A

Notes
• This version does not include the changes Firmware v1.12 and v1.13.
Applicable Products

Supported Operating Systems
N/A

New Features
N/A

Enhancements
• [Web] User cannot log in when a CSRF (Cross-Site Request Forgery) attack is detected.

Bugs Fixed
• [User Accounts] Backdoor account is transparent to unauthorized users.
• [Web] The same cookie is used when multiple users access the web page at the same time.
• [Web] Web server crashes if the HTTP POST command is in an invalid format.
• [Web] Web server crashes if a cookie is NULL for certain URLs.

Changes
N/A

Notes
N/A
**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- Supports up to 8 accounts and username can be modified.
- Supports two categories of users; Admin and User—Admin can read/write from/to configuration information and User is only allowed to read the configuration.
- [SNMP] The user account created first is the designated SNMP v3 account.
- [Web] A cookie is generated for each login.
- [Web] After sending out data through the web page, the web server only allows one user to send data back to safeguard against the CSRF (Cross-Site Request Forgery) Vulnerability.
- [Web] Alerts users to use HTTPS when changing passwords.
- [Web] Encrypts the password before transmitting it.

**Enhancements**
- Removes the backdoor account.

**Bugs Fixed**
- [Web] Some files/information accessible without users logging in.
- [Web] Browser will redirect to an invalid web page if the web page is tampered.
- [Web] Linux commands that are not allowed can be entered on the page and the web server will execute them.
- [Web] Web server crashes if the URL is invalid.

**Changes**
N/A

**Notes**
N/A
Applicable Products

Supported Operating Systems
N/A

New Features
- SNMP supports WLAN connection status and Client/Slave connecting time.
- Supports new regulations for CE certificate and EN 300 328 V1.9.1 standard.
- Supports the MXview Wireless Dashboard.
- KC and RCM certification.

Enhancements
- Default value setting of TX Power is 20 dBm.
- Modified the format for the associated client connection period from dd hh:mm:ss to seconds.

Bugs Fixed
- Kernel panic when AP serves over 120 clients simultaneously.
- Browser crash issue when there are too many web error messages.
- Channel information update issue on the overview page if the DFS channel changes when a radar signal is detected.
- SNR display issue on MXview.
- Fixed channel information update issue in the Sniffer mode.

Changes
- Removed "Disable" option for the WLAN operation mode in SNMP.

Notes
N/A
Applicable Products

Supported Operating Systems
N/A

New Features
• Added troubleshooting support for faster diagnostics (Maintenance > Troubleshooting).
• Added ARP Table, Bridge Status, LLDP Status, Routing Table, and RSTP Status.

Enhancements
• Limits the multicast traffic to 150M on Ethernet interface to avoid CPU overload.
• APs can now send gratuitous ARP to wireless clients after association.
• Updated the web UI to prevent Cross-Site Script (XSS) attack.
• Updated the WLAN function and changed the bmiss count from 5 to 10.
• Updated DFS function to raise radar SNR threshold to 30 for the FCC type 5 radar.
• Updated chpasswd encrypt method from DES to MD5 to increase the length of the password.
• Updated the format of the DHCP Client List.

Bugs Fixed
• Port setting failure in “TCP/UDP port filters”.
• Issues with AP IP address display on the wireless status page.
• Time Zone setup issue.
• Static DHCP mapping failure issue.

Changes
• Allows the selection of channel 14 in the JP model.
• Frees skb_buff when the bridge device isn't running to avoid memory leak.
• Improves the turbo roaming break time to < 150 ms when TKIP security is selected.
• Modifies the MAC Clone function to allow devices to take on the original Moxa MAC address when the cloned device is removed.

Notes
N/A
Applicable Products

Supported Operating Systems
N/A

New Features
• DFS channel support. Note: AP mode does not support channels 120, 124, and 128, but client mode supports these channels.
• Supports Client-based Turbo Roaming.
• Supports the Sniffer operation mode.

Enhancements
• WLAN stability improvements.
• Maximum wireless transmission power increased to be consistent with the hardware capability.
• Changed default value of minimum transmission rate from 13 Mbps to "0 - default disabled".
• LLDP uses device’s MAC as its source MAC, instead of Moxa-specified MAC: Format "00:90:E*:00:00:81".

Bugs Fixed
• UI Improvements.
• Improved the associated client list display and DHCP clients display tables.
• No antenna selection for Antenna A/B and Auto Mode.

Changes
• Changes to the network settings for LLDP.
• Removed the "short guard interval" setting.

Notes
N/A
<table>
<thead>
<tr>
<th>Version: v1.1</th>
<th>Build: Build 14071711</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Applicable Products**

**Supported Operating Systems**
N/A

**New Features**
- First release.

**Enhancements**
N/A

**Bugs Fixed**
N/A

**Changes**
N/A

**Notes**
N/A