Firmware for AWK-4131A Series Release Notes

Version: v1.15	Build: 20071510
Release Date: Jun 30, 2020	

Applicable Products

AWK-4131A series

Supported Operating Systems

N/A

New Features

• Added 8 channels (total 11) for Client-based Turbo Roaming channel scanning.
• Added support for Turbo Roaming in Slave Mode.
• Added support for AeroMag in Client-Router Mode.
• Added support for Wi-Fi Remote Connection Check.
• Added support for WDS.
• 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.
• Added client isolation in AP mode.

Enhancements

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

[AeroLink]
• Long break time when rebooting the AP or Client.

Bugs Fixed

[WLAN]
• The AP responds to unicast probe requests, even if the AP is not the receiver.
• The GARP reply sent by the AP/Client does not have a VLAN tag.
• Unable to establish a Wi-Fi connection with APs that support 802.11r.
• G-mode-only clients are unable to associate with the AP.
• Authentication may fail when the client's security is set to Enterprise mode.
• The BSS node is cleaned in Master mode.

[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.

[Security]
• The Wireless Search Utility cannot find clients that use the 4th WEP key.
• CVE-2018-10694: The open "wireless interface" is enabled by default which can be exploited by unauthorized users.
• CVE-2018-10698: TELNET is enabled by default.
• CVE-2018-10690: HTTP is enabled and HTTPS is disabled by default.
• CVE-2018-10692: The session cookie does not have an HttpOnly flag.
• CVE-2018-10695: The send email to admin account function can be used to execute Linux commands on the device.
• CVE-2019-5136: Improper system access as a higher privilege user, an attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.
• CVE-2019-5137: Exploitable Hard-coded Cryptographic Key allows for the decryption of captured traffic.
• CVE-2019-5138/CVE-2019-5140/CVE-2019-5141/CVE-2019-5142: Improper Neutralization of Special Elements used in an OS Command.
• CVE-2019-5139: Exploitable hard-coded credentials.
• CVE-2019-5143: Buffer Copy without Checking Size of Inpup may cause remote code execution.
• CVE-2019-5148: An attacker can send a crafted packet and cause denial-of-service of the device.
• CVE-2019-5153: Stack-based Buffer Overflow.
• CVE-2019-5162: Improper remote shell access to the device, an attacker can send commands while authenticated as a low privilege user to trigger this vulnerability.
• CVE-2019-5165: An exploitable authentication bypass vulnerability, an attacker can trigger authentication bypass on specially configured device.

[WEB]
• Specifying the max byte size of the primary RADIUS shared key will change the setting of the secondary RADIUS server IP.
• Unable to set VAP3 to VAP9 as the RF-type for A/N Mixed mode, Channel 36, and channel width 20/40 MHz.
• Wi-Fi channel selection does not work properly on Quick Setup.
• The web server crashes when reading invalid content.

[DHCP]
• The number of DHCP server users cannot be set to more than 128.
• The DHCP server does not work properly when AeroMag AP enabled.

[Config]
• 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.

[AeroMag]
• The master AP is unable to receive packets, causing group failure.
• AeroMag Clients fail to initialize the configuration received from the AeroMag AP.
• The WLAN LED turns off when renewing configuration settings or refreshing channels.
• Resetting to default settings does not clean AeroMag configuration files.
• AeroMag AP can only serve 7 VAPs.
• The AeroMag Client page is blank during Quick Setup.
• Unable to configure AeroMag after performing a channel analysis.

[Firewall]
• IP filter does not drop packets if MAC filtering is disabled.
• 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 would sometimes cause a memory leak.

[MXview]
• Unable to import or export configuration files and upgrade firmware using MXview.

Changes

[WLAN]
• Changed the default multicast rate value.
• Changed the fix rate list according to the selected RF type.
• Changed the management frame rate according to the selected RF type.
• Changed the number of management frame transmission retries from 8 to 4.
• Changed the basic rate of G-only mode to be same rate as 802.11b.

[Security]
• CVE-2018-10694: The open "wireless interface" is now disabled by default.

[Firewall]
• Increased MAC/IP/Port filter entries up to 60.
• Changed the default rule policy to ACCEPT.

[WEB]
• Changed the default system description to the model name.
• Changed the web configuration import buffer size from 64K to 128K.
• ser-level accounts can now no longer see other user account information.

[LED]
• Adjusted the Wi-Fi signal level LED.

Notes

This firmware version is currently incompatible with the officially released versions of Wireless Search Utility v2.6, MXConfig v2.6, and MXview v3.1. These utilities are expected to be updated to support this firmware version in Q4 2020. For urgent cases that require these utilities to be used with this firmware, please contact MOXA technical support for access to the beta version of these

Version: v1.13	Build: Build_18121215
Release Date: Dec 26, 2018	

Applicable Products

AWK-3131A-JP-T, AWK-4131A-US-T, AWK-4131A-JP-T, AWK-3131A-US, AWK-4131A-EU-T, AWK-3131A-JP, AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US-T

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 standards.
- Issue with the error handler for abnormal Wi-Fi packets
- Static route of WLAN iface does not work for DHCP client in Client-Router mode

Changes

N/A

Notes

N/A

Version: v1.12	Build: Build_18090617
Release Date: Oct 30, 2018	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• DFS: Abnormal behavior of DFS function.

Changes

• AeroMag: Hides the unnecessary SSID when AWK is configured as an AeroMag AP.

Notes

N/A

Version: v1.11	Build: Build_18062617
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

- [AeroMag] Supports AeroMag client.
- [NAT] Supports 1-to-1 NAT.
- [DHCP client] Supports DHCP option 12 (hostname = device name).
- [DHCP client] Supports DHCP option 50 (requested IP address).
- [Network Status] Provides bridge status via SNMP.

Enhancements

- WLAN: Supports the WLAN system log version 2.
- AeroMag: Adds system log for channel analysis and applying the configuration.
- MAC clone: Adds system log for MAC clone.
- Quick setup: If RF type is pure N, WEP is not supported.
- Quick setup: Adds WEP length checker for WEP security.
- Quick setup: Supports TKIP on B/G/BGMixed/A only.
- Quick setup: If RF type is pure N, AES/TKIP mixed is not supported.

Bugs Fixed

- WLAN:Rx stuck issue.
- WLAN: Tx hang caused by interrupt (0x0000 0000) messages.
- WLAN: DUT reboots if it roams for many times.
- WLAN: AP always works on 20 MHz, if there is an another AP on the specified channel when it booting up.
- WLAN: AP with multiple VAPs just only works on 20 MHz, even if its bandwidth is configured at 20/40MHz.
- WLAN: GARP is not sent out, if driver cannot get the interface IP or cannot allocate malloc (skb).
- WLAN Status: Value of WLAN assoc rx/tx pkts/bytes always is 2147483647, if the value is over 2147483647.
- Turbo roaming: Unexpected roaming occurs because the AP Alive check timer resumes after receiving packets on a foreign channel.
- Turbo roaming: The AP candidate threshold is not effective when both the AP alive check and Client-based Turbo Roaming ere enabled.
- Turbo roaming: Roaming log has wrong SNR.
- AeroMag: Web console cannot get the latest information after channel refresh or reconfigure.
- AeroMag: MAC Clone does not work after applying the new configuration.
- AeroMag: AeroMag AP assigns configuration to other devices in the same group before regenerating a new configuration.
- RSSI report: Scanned node which is not updated for 1 sec is not included in the report.
- RSSI report: Facility and severity parameters in the RSSI report are inot correct.
- RSSI report: Noise/SNR values are sometimes inaccurate.
- Configuration: Cannot change the bandwidth to 20/40MHz in client mode in some cases.
- WEB: Login message should use the activated configuration.
- WEB: Length of SSID can’t be longer than 32.
- WEB: Cannot input 240 characters in web login message and login authentication failure message.

• WEB: UI does not show unit of the roaming threshold (SNR).
• WEB: System log cannot be exported via Firefox 59.0.223.
• WEB: Cannot enable Turbo Roaming via web UI, if RF type is 2.4G type.
• WEB: Linux command can be injected in POST data commands.
• WEB: Web server crash, if user modifies the password during login.
• WEB: User can't increase the minimum length of the password, if current password is less than the specific length.
• WEB: User-level user can't use "Diagnostics" and "Wi-Fi Mirror Port".
• WEB: User-lever user can't export current device information on Troubleshooting page.
• Utility: Cannot reboot the device through MXconfig.

Changes

• MAC Clone: Changes the STA MAC to the MAC of the backend PC, even if it has not connected to the AP.
• Configuration: To enhance RX accuracy, new roaming configuration is created to replace the current configuration; "AP candidate threshold" configurations are different from legacy mode, 2.4GN-related mode, and 5GN-related mode.
• Configuration: Changed the range of "Inactive timeout" from 1 -240 seconds to 8-240 seconds in AP mode.
• Configuration: Operation mode is changed automatically once AeroMag is enabled.
• Configuration: Changed the max length of user's password from 16 to 32.
• Configuration: SNMP settings includes secondaryKey1, ro_community, and rw_community; settings will be encrypted in exported configuration.
• DHCP Client: Initial network IP is set to 169.254.0.1 before getting an IP from DHCP for the 1st time.
• Network Settings: Device IP shall not be the network ID.
• WEB/Utility: Network information can’t be the current IP/netmask/Gateway when AWK acts as a DHCP client.
• WEB: Disabled all buttons when the logs on the system log page are cleared.
• WEB: Add "Skip" option where user is asked to modify the password on login page.
• Troubleshooting: Changed all the special characters in file name except dash to underscore.

Notes

N/A

Version: v1.10	Build: Build_18032720
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• CVE-2017-14459; Telnet, Serial console, SSH will reject invalid characters to prevent injection attacks.

Changes

N/A

Notes

N/A

Version: v1.9	Build: Build_18012818
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• Web server will reject invalid characters including ` ' " | ; &

Changes

• Changes the format of device name to AWK-3131A_[the last six digits of MAC address].
• Shows complete S/N information.

Notes

N/A

Version: v1.8	Build: Build_17122516
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

• Supports Wi-Fi Mirror Port.
• Supports AeroLink Protection with SNR check.
• Supports AeroLink Protection with VLAN.
• Supports the SNR/Noise floor on MXview dashboard.

Enhancements

• Optimized the roaming recovery time for the scenario that 4-4 EAPOL packet is dropped.
• Optimized the packets lost under following two conditions: Master and Slave connection under 802.11n mode and WPA/WPA2, the traffic comes behind Master to the slave and the devices behind the slave at the same time.

Bugs Fixed

• Wi-Fi client signal strength is not correct and not accessible after connected AP disappeared.
• Syslog server still work while server port is not assigned.
• Roaming event is recorded as connection event, if the first bytes of AP's MAC is 0x00.
• If the operation mode is client-router, AWK could not use WPA/WPA2 enterprise mode.
• If AP using channel 140 changes to client mode, channel width cannot be set to 20/40.
• User cannot access web console if AWK received IP again from DHCP server.
• If the AWK is DHCP client and enables MAC clone, AWK cannot receive the IP from Cisco AP and then Cisco AP will disconnect AWK.
• Network looping causes AeroLink Projection works abnormally.
• AeroLink does not support slave mode.
• If the roaming message is larger than 128 bytes, the some syslog messages are missing.
• The maximum transmission power is allow to set the value which is out of the valid range.
• Error message for account settings is incorrect if account name is duplicated.
• The cookie paring is incorrect.
• Cannot retrieve information via OneKeyInfo.
• AWK cannot reboot and configure via MXconfig under some circumstances.
• If the size of configured value is larger than 64 bytes, the configuration setting will not succeed.

Changes

• Does not support the configuration 0 for all TCP/UDP port settings (TCP/UDP 0 port is a reserved port).

Notes

N/A

Version: v1.7	Build: Build_17102616
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

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

Version: v1.6	Build: Build 17091517
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

- Supports AeroMag.
- Supports quick setup.
- Supports Moxa security level 1.
- Supports WPA/WPA2 Mixed.
- Supports Trouble shooting.
- Supports management encryption.
- Master mode supports multiple slaves.
- Supports Enable/Disable Ethernet LAN interface.
- Supports static MAC Clone.
- Supports channel 120 to 128 in US model.

Enhancements

- 802.3az is not supported.
- [SNMP] Use iface speed as ifHighSpeed on ifXTable.
- [Web] Do not show inactive timeout in client-router mode.
- LLDP does not support 802.3.
- Encrypt/Decrypt Remote Protocol data payload.
- [LLDP] Delete the 1000baseT_Half/1000baseT_Full when the AR934x_ETH_FAST feature enable on the mvport ethtool.
- Porting OpenSSL 1.1.0e is supported.
- Change roaming threshold default value to -65 under legacy mode, -55 under 2.4 GHz N mode, and to -50 under 5 GHz N mode
- Max TX Power changes as following.

Bugs Fixed

- Issue with simultaneous RF type mixed mode connectivity to different pure RF type modes.
- Rebooting issue while scanning DFS.
- Boot up failure issue.
- Interoperability with Cisco/Aruba/Ruckus AP by sending EAPOL frame with QOS data.
- Ping web console page attack from unknown commands.
- Rx stuck by patching qca-wifi-10.4 (QSDK).
- AP kernel panic when 128 clients connect and some clients are trying to reconnect.
- CCA will reset to default when channel changed.
- Roaming with multicast traffic will causing client cannot connect issue.
- Abnormal roaming time recorded in system log when client connection fail.
- Multi-channel roaming fail issue.
- Fixed bmiss will not trigger while bgscan due to bmiss counter reset issue.
- RSSI report format incorrect.
- rror when old log version upgrade to the new log version.
- RSTP looping because of no preroot_port.
- RSTP recovery too long issue and web display bug.
- SNMP cannot provide wireless status information.

• Loading the file which cannot be decrypted would cause iw_web crash.
• Incorrect interface name on LLDP status page and incorrect device name on bridge table page issue.
• Setting the LAN IP failed when the client-router mode via wireless search utility.
• ifXTable has null vale on SNMP.
• Web console has incorrect information under client-router mode
• Kernel panic while Turbo roaming is enabled.
• Kernel panic while interface is cannot fetch noise floor at the same time.
• Turbo Roaming chooses next AP with accurate roaming difference.
• MAC Clone should not be assigned as the multicast address.
• If DUT is in sniffer mode, device behind Ethernet cannot access DUT.
• Kernel panic while detecting specific DFS signal.
• Incomplete record of LFPT event in system log.
• Incorrect antenna selection under client mode.
• SNMP NID not correct.
• lients using enterprise mode cannot reconnect while AP reboots.
• IP setting issue via wireless search utility under client-router mode.
• Incorrect TX power information on the web console.
• Incorrect Wi-Fi driver state machine.
• Cannot import decrypted configuration.
• Issue finding AP with hidden node while turbo roaming is triggered.

Changes

N/A

Notes

N/A

Version: v1.5	Build: Build 17041601
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

- [Web] Login denied when CSRF (Cross-Site Request Forgery) attack is detected.

Bugs Fixed

- [Accounts] Backdoor account is transparent to unauthorized users.
- [Wireless Search Utility] Service crash during data encryption for some commands.
- [Web] Cookies are same when multiple users access the website at the same time.
- [Web] Web server crash, if the HTTP POST is in invalid format.
- [Web] Web server crash, if the cookie is NULL for some URLs.

Changes

N/A

Notes

N/A

Version: v1.4	Build: Build 17031018
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

• [Accounts] Supports 8 accounts, including Administrators and normal users; administrators can read/write all settings, users are only allowed to read information.
• [SNMP] AWK uses the first account (list in the first entry) out of 8 accounts for your SNMP v3.
• [Web] Cookie is generated every time users login.
• [Web] Web server only allows one user to send the data back to avoid CSRF (Cross-Site Request Forgery) Vulnerability.
• [Web] A warning message suggesting using HTTPS is displayed when user is changing password via HTTP.
• [Web] Encrypts password, before transmitting it.
• [Wireless Search Utility] Encrypts the data between the device and Wireless Search Utility.

Enhancements

• Default password changes from root to moxa.

Bugs Fixed

• [Web] File/information accessible even if user does not log in.
• [Web] Browser will redirect to invalid web page, if the web page is tampered.
• [Web] Unauthorized Linux commands can be run via the webpage.
• [Web] Web server crash if the URL is invalid.

Changes

N/A

Notes

N/A

Version: v1.3	Build: Build 16100315
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T, AWK-4131A-EU-T, AWK-4131A-US-T, AWK-4131A-JP-T

Supported Operating Systems

N/A

New Features

- SNMP supports WLAN connection status and Client/Slave connecting time.
- Supports new regulatory standards of CE certificate and EN 300 328 V1.9.1.
- KC and RCM certification.
- Supports MXview Wireless Dashboard.

Enhancements

- SNMP does not support "Disable" for WLAN operation mode.
- Default value setting of TX Power is 20dBm.

Bugs Fixed

- Kernel panic when AP serves over 120 clients simultaneously.
- Web crash when there are too many web error messages.
- Channel information on overview page not updated when DFS channel changes.
- SNR information issue in MXview.
- Channel information issue in Sniffer mode.

Changes

N/A

Notes

N/A

Version: v1.1	Build: Build 15122211
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T

Supported Operating Systems

N/A

New Features

• [Channel] 5 GHz DFS channel support.
• [Distance] 5 GHz long-distance communication support.
• [Diagnostics] One-key information support.
• [Network Status] ARP Table, Bridge Status, LLDP Status, Routing Table, and RSTP Status.

Enhancements

• Increased the Tx buffer from 1024 to 4096.
• Modified Rx Packet Count (ATHR_RX_PKTS_CNT) to 100 and number of Rx Packet (AG7240_NUMBER_RX_PKTS) to 4096.
• Removed "select all" checkboxes in all "lkogs and Notification" pages.
• Shows SNTP in a string instead of a selection box if "IWCONFIG_SUPPORT_NTF" is not set and there's only one time-protocol option.
• Changed the "Restart" logo.

Bugs Fixed

N/A

Changes

• Kernel panic when AP serves over 120 Client at the same time.
• Web crash when there are too many web error messages.
• Fixed the channel information on Overview page when the DFS channel keeps changing.
• Issue with the SNR information in MXview.
• Issue with channel information in Sniffer mode.

Notes

N/A

Version: v1.0	Build: Build 15061120
Release Date: N/A	

Applicable Products

AWK-3131A-EU, AWK-3131A-EU-T, AWK-3131A-US, AWK-3131A-US-T, AWK-3131A-JP, AWK-3131A-JP-T

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A