Firmware for AWK-1131A Series Release Notes

Version: v1.22	Build: 21030515
Release Date: Apr 01, 2021	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added an option to keep wireless enabled when resetting the AWK back to factory default settings.

Enhancements

N/A

Bugs Fixed

• The AP's address does not show in the web interface when in Client mode.
• Third-party clients connecting to the AWK AP would cause a kernel panic.
• The AWK does not send GARP packets after connecting to the next AP in Client-Router mode.
• Clients that roamed from AP1 to AP2 still exist in AP1's associated clients list.

Changes

N/A

Notes

N/A

Version: v1.21	Build: 20071510
Release Date: Jun 30, 2020	

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.
• Added client isolation in AP mode.

Enhancements

[WLAN]
• When in Client Mode, the AWK now takes less time to reconnect after being disconnected by the AP.
• When in Client Mode, the AWK now takes less time to reconnect if MAC Clone is enabled.
• When in Client Mode, the AWK now takes less time to reconnect if the second EAPOL packet is lost.
• When in Client Mode, the AWK now takes 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.
• 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.

[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: v1.19	Build: Build_18121212
Release Date: Dec 28, 2018	

Applicable Products

AWK-1131A-JP-T, AWK-1131A-EU, AWK-1131A-US, AWK-1131A-US-T, AWK-1131A-EU-T, AWK-1131A-JP

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

Version: v1.18	Build: Build_18100315
Release Date: Oct 30, 2018	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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

Version: v1.17	Build: Build_18072017
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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

Version: v1.16	Build: Build_17102617
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-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: v1.15	Build: Build 17101216
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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.

Version: v1.14	Build: Build 17081814
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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.

Version: v1.13	Build: Build 17041601
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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.
• [Wireless Search Utility] Services crash during data encryption for certain commands.
• [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

Version: v1.12	Build: Build 17031018
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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.
• [Wireless Search Utility] Encrypts data transferred between devices and the Wireless Search Utility.

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

Version: v1.11	Build: Build 16100315
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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

Version: v1.10	Build: Build 16022214
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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

Version: v1.8	Build: Build 15061212
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

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

Version: v1.1	Build: Build 14071711
Release Date: N/A	

Applicable Products

AWK-1131A-EU, AWK-1131A-US, AWK-1131A-JP, AWK-1131A-EU-T, AWK-1131A-US-T, AWK-1131A-JP-T

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A