Firmware for AWK-3251A-RCC Series Release Notes

Version: v2.0	Build: 2025_1002_2200
Release Date: Feb 02, 2026	

Applicable Products

AWK-3251A-RCC Series

Supported Operating Systems

N/A

New Features

- Added support for Fast Bootup.
- Added support for AP-based Disconnection.
- Added support for Link Fault Pass-through.
- Added support for Wi-Fi ACL.
- Added support for IPv6 Configuration.
- Added support for DHCPv6 Server.
- Added support for Certificate Management.
- Added support for Security Status.
- Added support for RSSI Reporting.

Enhancements

- Improved the performance, security, and stability of Wi-Fi Mirroring.
- Improved the stability and performance of Auto Carriage Connection (ACC).
- Added a signature option to the diagnostics function to improve security.
- Centralized socket cleanup to prevent resource leaks.
- Upgraded musl to V1.1.24.
- Upgraded OpenSSL to 1.1.1za.
- Upgraded OpenSSH to 10.0p1.
- Added One Key information to the bridge fdb command.

Bugs Fixed

- Remote host check behaves abnormally in Client-router and Slave mode.
- The RADIUS server is unreachable via SSH.
- The displayed TX rate information does not match the software specification.
- The Wi-Fi interface fails to initialize in channel 116/140 when using certain country codes that support this channel.
- The antenna configuration and status values do not match.
- When using WPA3 encryption, the device times out when roaming to an AP it has never connected to before.
- The 802.11w settings for WPA2/WPA3 Mixed mode are incorrect.
- Clients disconnect despite receiving probe responses.
- The Wi-Fi driver may unexpectedly stop working.
- The system shows incorrect LAN interface information for LFPT.
- Users cannot access the Wireless settings page if the SSID contains an asterisk.
- Changes fail to apply when setting the channel to 36 on the RF Settings page.
- Excessive configuration changes may cause the VLAN to abruptly reload.
- The L2 firewall behaves abnormally.
- Users are unable to configure the same port as the firewall start and end port.
- The IP management configuration shows incorrectly in Client-router mode.

- Users cannot set channel width 20/40 or 20/40/80 (5 GHz).
- The 2.4 GHz TX power information shows incorrectly when using certain country codes.
- The Wi-Fi SSID Status table times out when too many VAPs are enabled.
- Users cannot configure SSIDs that consist solely out of numbers and exceed 10 characters via the CLI.
- Requesting the client status via CLI does not work.
- If the SSID name contains a space, relevant wireless, interface, and VLAN CLI commands do not work.
- The system incorrectly shows DHCP IP change error messages when the DHCP server is disabled.
- Configuring the device IP may reset it to the default value.
- The AP MAC address is not recorded in the event log when AP Alive Check fails.
- When roaming, the device chooses the nearest AP instead of the AP with the best signal.
- CVE STA kernal panic vulnerability issue.
- CVE-2023-5216 vulnerability issue.
- CVE-2020-24586 vulnerability issue.
- CVE-2020-24587 vulnerability issue.
- CVE-2020-24588 vulnerability issue.
- CVE-2020-26139 vulnerability issue.
- CVE-2020-26140 vulnerability issue.
- CVE-2020-26141 vulnerability issue.
- CVE-2020-26142 vulnerability issue.
- CVE-2020-26143 vulnerability issue.
- CVE-2020-26144 vulnerability issue.
- CVE-2020-26145 vulnerability issue.
- CVE-2020-26146 vulnerability issue.
- CVE-2020-26147 vulnerability issue.
- CVE-2021-0920 vulnerability issue.
- CVE-2023-3772 vulnerability issue.
- CVE-2021-0512 vulnerability issue.
- CVE-2022-30594 vulnerability issue.
- CVE-2022-29581 vulnerability issue.
- CVE-2022-28356 vulnerability issue.
- CVE-2022-27223 vulnerability issue.
- CVE-2022-24958 vulnerability issue.
- CVE-2022-1353 vulnerability issue.
- CVE-2022-0492 vulnerability issue.
- CVE-2021-45485 vulnerability issue.

- CVE-2021-4197 vulnerability issue.
- CVE-2021-4083 vulnerability issue.
- CVE-2021-40490 vulnerability issue.
- CVE-2021-39698 vulnerability issue.
- CVE-2021-39685 vulnerability issue.
- CVE-2021-39634 vulnerability issue.
- CVE-2021-37159 vulnerability issue.
- CVE-2021-3715 vulnerability issue.
- CVE-2021-29154 vulnerability issue.
- CVE-2021-22555 vulnerability issue.
- CVE-2020-8648 vulnerability issue.
- CVE-2020-35508 vulnerability issue.
- CVE-2020-29660 vulnerability issue.
- CVE-2020-29374 vulnerability issue.
- CVE-2020-28974 vulnerability issue.
- CVE-2020-25705 vulnerability issue.
- CVE-2020-25668 vulnerability issue.
- CVE-2020-25285 vulnerability issue.
- CVE-2020-25211 vulnerability issue.
- CVE-2020-16166 vulnerability issue.
- CVE-2020-15436 vulnerability issue.
- CVE-2020-14381 vulnerability issue.
- CVE-2020-14351 vulnerability issue.
- CVE-2020-14305 vulnerability issue.
- CVE-2020-13974 vulnerability issue.
- CVE-2020-12464 vulnerability issue.
- CVE-2020-11565 vulnerability issue.
- CVE-2020-10711 vulnerability issue.
- CVE-2020-0466 vulnerability issue.
- CVE-2020-0465 vulnerability issue.
- CVE-2020-0444 vulnerability issue.
- CVE-2020-0433 vulnerability issue.
- CVE-2020-0431 vulnerability issue.
- CVE-2019-20636 vulnerability issue.
- CVE-2019-2054 vulnerability issue.
- CVE-2019-19768 vulnerability issue.
- CVE-2019-19447 vulnerability issue.

- CVE-2019-19319 vulnerability issue.
- CVE-2019-18805 vulnerability issue.
- CVE-2019-17133 vulnerability issue.
- CVE-2019-16746 vulnerability issue.
- CVE-2019-15916 vulnerability issue.
- CVE-2019-15807 vulnerability issue.
- CVE-2019-15666 vulnerability issue.
- CVE-2019-13272 vulnerability issue.
- CVE-2019-11479 vulnerability issue.
- CVE-2019-11478 vulnerability issue.
- CVE-2019-11477 vulnerability issue.
- CVE-2019-10639 vulnerability issue.
- CVE-2019-0136 vulnerability issue.
- CVE-2018-9568 vulnerability issue.
- CVE-2018-9517 vulnerability issue.
- CVE-2018-9516 vulnerability issue.
- CVE-2018-9415 vulnerability issue.
- CVE-2018-8897 vulnerability issue.
- CVE-2018-5873 vulnerability issue.
- CVE-2018-5391 vulnerability issue.
- CVE-2018-25020 vulnerability issue.
- CVE-2018-20961 vulnerability issue.
- CVE-2018-20856 vulnerability issue.
- CVE-2018-20836 vulnerability issue.
- CVE-2018-20169 vulnerability issue.
- CVE-2018-18559 vulnerability issue.
- CVE-2018-17182 vulnerability issue.
- CVE-2018-14634 vulnerability issue.
- CVE-2018-10938 vulnerability issue.
- CVE-2018-1093 vulnerability issue.
- CVE-2018-1092 vulnerability issue.
- CVE-2018-10880 vulnerability issue.
- CVE-2018-10879 vulnerability issue.
- CVE-2018-10878 vulnerability issue.
- CVE-2018-1068 vulnerability issue.
- CVE-2018-10675 vulnerability issue.
- CVE-2017-15951 vulnerability issue.

- CVE-2017-9074 vulnerability issue.
- CVE-2017-7889 vulnerability issue.
- CVE-2017-7618 vulnerability issue.
- CVE-2017-7308 vulnerability issue.
- CVE-2017-6001 vulnerability issue.
- CVE-2017-18595 vulnerability issue.
- CVE-2017-18509 vulnerability issue.
- CVE-2017-18255 vulnerability issue.
- CVE-2017-18079 vulnerability issue.
- CVE-2017-18017 vulnerability issue.
- CVE-2017-17558 vulnerability issue.
- CVE-2017-17450 vulnerability issue.
- CVE-2017-17448 vulnerability issue.
- CVE-2017-16995 vulnerability issue.
- CVE-2017-16939 vulnerability issue.
- CVE-2017-15649 vulnerability issue.
- CVE-2017-12762 vulnerability issue.
- CVE-2017-11472 vulnerability issue.
- CVE-2017-11176 vulnerability issue.
- CVE-2017-1000407 vulnerability issue.
- CVE-2017-1000405 vulnerability issue.
- CVE-2017-1000370 vulnerability issue.
- CVE-2017-1000371 vulnerability issue.
- CVE-2017-1000365 vulnerability issue.
- CVE-2017-1000364 vulnerability issue.
- CVE-2017-1000363 vulnerability issue.
- CVE-2017-1000111 vulnerability issue.

Changes

- Increased the Locator timeout threshold from 300 to 3600 seconds.
- DHCP Client has been synced with the Wi-Fi 4 Series.
- Removed the debug log from the management frame.

Notes

N/A

Version: v1.0	Build: 2023_0330_1326
Release Date: Aug 16, 2023	

Applicable Products

AWK-3251A-M12-RCC-UN, AWK-3251A-M12-RCC-UN-CT-T, AWK-3251A-M12-RCC-UN-T, AWK-3251A-M12-RCC-US, AWK-3251A-M12-RCC-US-CT-T, AWK-3251A-M12-RCC-US-T

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A