Firmware for AIG-101 Series Release Notes

Version: v1.3.0	Build: N/A
Release Date: Nov 04, 2025	

Applicable Products

AIG-101 Series

Supported Operating Systems

Moxa Industrial Linux 1 (Debian 9)

New Features

N/A

Enhancements

• RED Cybersecurity EN18031-1 compliance.

To adopt RED Cybersecurity EN18031-1, the AIG includes the changes below:
- HTTPS connection now only supports TLS v1.2 or higher.
- HTTP redirect to HTTPS service now is enabled as default
- Force to modify the admin's password upon the first login
- Remove the default password for the Wi-Fi AP feature

• The DLM Client for the Moxa DLM Service now implements a backoff mechanism to prevent excessive message repetition during high-frequency events, optimizing events reported while ensuring critical notifications remain visible.
?- If the same event occurs five times within a 5-minute window, the system enters backoff mode, progressively increasing the message delay up to a maximum of 60 minutes.
?- During backoff, events are sent as compressed messages with an indication of suppression count (e.g., "backed off for x times").
?- Normal message delivery is resumed once the event stops occurring or after a device reboot.

Bugs Fixed

• When the WAN connection was restored by replugging the Ethernet cable, the connection to the AWS IoT Core service was not re-established.
• The certificat weren't received properly after the AIG was fully registered, and the Moxa DLM Service returned error code 500.
• The tag type changed from uint16 to double when the scalingFunc in the exported Modbus CSV file was set to 1 and then imported again.
• The upgrade from v1.1 to v1.2 in an offline environment failed because the dependency package curl was not prebuilt.

Changes

• Upgrade Azure IoT Device SDK to LTS_03_2025.
• When no DNS information is received on the cellular interface, treat the network as connected. Note that this may affect the Cellular Enable check-alive mechanism. Ensure that a reachable target host is properly configured to prevent the check-alive process from looping.

Notes

• Tag Dashboard Value Precision Issue

The tag monitor may display incorrect values when handling numbers beyond JavaScript’s safe integer range (±2^53 ? 1, i.e., from ?9,007,199,254,740,991 to 9,007,199,254,740,991).

This is due to a limitation in JavaScript number precision. When values such as int64 or uint64 exceed this range, browsers (e.g., Chrome) will show distorted results when parsing JSON raw data.

• Upgrade From the Local Drive: To upload the upgrade package requires a minimum upload speed of 1MB/sec.
• The upgrade process from firmware v1.2.0 to v1.3.0 will require approximately 20+ minutes.

Version: v1.2	**Build: N/A**
Release Date: Nov 14, 2024	

Applicable Products

AIG-101 Series

Supported Operating Systems

Moxa Industrial Linux 1 (Debian 9)

New Features

• Supports backup of logs with FTP/SFTP upload capability.

Enhancements

N/A

Bugs Fixed

• When the number of tags is too large, the Web UI may crash.
• OpenVPN disconnection and reconnection issues.
• Incorrect maximum journal log size limit.
• An issue of the DLM service not being registered.
• Using Auto Arrange function may cause the Modbus slave to crash.
• An issue of GPS time synchronization drift.
• A tag streaming issue during Modbus device disconnection and reconnection wherein the tag was not updated.
• When UPort is disconnected, the UPort status on Tag Management is not synchronized.
• After scanning for ioLogik, clicking on it may cause the web UI to crash.
• Incorrect information displayed by the Modbus slave diagnostic function.
• An instance where memory usage was unusually high.
• A module connection failure issue when the UDP DNS payload was too long.
• An issue where the GPS API did not return up-to-date values.
• An issue of apps failing to start after a reboot.
• CVE-2024-1086: https://nvd.nist.gov/vuln/detail/CVE-2024-1086.
• CVE-2024-21646: https://nvd.nist.gov/vuln/detail/CVE-2024-21646.
• CVE-2024-27099: https://nvd.nist.gov/vuln/detail/CVE-2024-27099.
• CVE-2024-25110: https://nvd.nist.gov/vuln/detail/CVE-2024-25110.

Changes

N/A

Notes

• The size of the upgrade package is approximately 250 MB. The upgrade process might require a minimum of 40 minutes.