

Product Change Notification—PCN# PCN000 001150**November 21, 2025**

Dear Valued Customer,

We would like to inform you that Moxa is going to make changes to the AIG-101, AIG-301, and AIG-501 Series. These changes will be implemented by November 21, 2025. Please review the details below to determine how these changes will affect your products and/or operations.

What will change?**AIG-101 V1.3.0****New Features**

N/A

Fixed Issues

1. When the WAN connection was restored by replugging the Ethernet cable, the connection to the AWS IoT Core service was not re-established.
2. The certificate wasn't received properly after the AIG was fully registered, and the Moxa DLM Service returned error code 500.
3. 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.
4. The upgrade from v1.1 to v1.2 in an offline environment failed because the dependency package curl was not prebuilt.

Enhancements

1. RED Cybersecurity EN18031-1 compliance.
To adopt RED Cybersecurity EN18031-1, the AIG includes the changes below:
 - HTTPS connections now only support TLS v1.2 or higher.
 - HTTP redirect to HTTPS service is now enabled as default
 - Forced to modify the admin's password upon the first login
 - Remove the default password for the Wi-Fi AP feature
2. The DLM Client for the Moxa DLM Service now implements a back-off 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 back off mode, progressively increasing the message delay up to a maximum of 60 minutes.

- During back off, events are sent as compressed messages with an indication of suppression count (e.g., "backed off for x times").
- Normal message delivery resumes when the event stops or the device reboots.

Changes

1. Upgrade Azure IoT Device SDK to LTS_03_2025.
2. 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

1. Tag Dashboard Value Precision Issue
The tag monitor may display incorrect values when handling numbers beyond JavaScript's safe integer range ($\pm 2^{53} - 1$, i.e., from -9,007,199,254,740,991 to 9,007,199,254,740,991).

This is because of 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.

2. Upgrading from the local drive to upload the upgrade package requires a minimum upload speed of 1MB/sec.
3. The upgrade process from firmware v1.2.0 to v1.3.0 requires approximately 20+ minutes.

AIG-301 V1.8.0

New Features

N/A

Enhancements

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

Fixed Issues

1. When the WAN connection was restored by re-plugging the Ethernet cable, the connection to the AWS IoT Core service was not re-established.
2. The certificate wasn't received properly after the AIG was fully registered, and the Moxa DLM

Service returned error code **500**.

3. 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.
4. Upgrading thingspro-agent to v2.3.0 extended the Azure IoT Edge module token refresh interval to reduce disconnection risks.
5. Failed to establish a 2G cellular connection in the EU.
6. The DO value didn't refresh immediately when the tag value had been modified.

Changes

1. Upgrade Azure IoT Device SDK to LTS_03_2025.
2. 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.
3. Sensitive and confidential data under the ThingsPro folder is now protected by permission control. Unauthorized users cannot read, write, or execute such data.
4. OPC UA Server changes:
 - The OPC UA server now generates X.509 private keys with a length of 2048 bits.
 - The signing algorithm has been upgraded to SHA-256.
 - Existing OPC UA server certificates will continue to be used. The new key length and algorithm apply only to certificates generated after the v1.8.0 upgrade.
 - The OPC UA server no longer includes any default or built-in user accounts.
 - User account information is now excluded from the OPC UA server's configuration import/export operations.
5. The Wi-Fi AP feature no longer ships with a default password.
6. Function changes:
 - The function (container) has been upgraded from Python 3.9 to Python 3.10.8
 - For Python package migration, the system will automatically reinstall the user's desired packages with network access; or you can call GET /api/v1/function/requirements/migration to retrieve the list of desired packages without network access. To provide flexibility, new APIs are available to manage the migration process:
 - i. **GET /api/v1/function/requirements/migration**: Fetch current settings, migration results, and desired packages.
 - ii. **PUT /api/v1/function/requirements/migration**: Update settings (e.g., enable/disable migration, timeout duration).

Notes

1. Tag dashboard value precision issue
The tag monitor may display incorrect values when handling numbers beyond JavaScript's safe

integer range ($\pm 2^{53} - 1$, i.e., from -9,007,199,254,740,991 to 9,007,199,254,740,991).

This is because of 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.

2. Upgrading from the local drive to upload the upgrade package requires a minimum upload speed of 1MB/sec.
3. The OPC UA Server certificate generation may rarely fail because of a race condition, which may be triggered if the apply operation is executed immediately after the regeneration operation in very quick succession. Perform an enable/disable OPC UA Server cycle to restore normal operations.
4. The upgrade process from firmware v1.7.0 to v1.8.0 requires approximately 20+ minutes.

AIG-501 V1.5.0

New Features

N/A

Enhancements

1. RED Cybersecurity EN18031-1 compliance.
To adopt RED Cybersecurity EN18031-1, the AIG includes the changes below:
 - HTTPS connections now only support TLS v1.2 or higher.
 - HTTP redirect to HTTPS service is now enabled as the default
 - Forced to modify the admin's password upon the first login
 - Remove the default password for the Wi-Fi AP feature
2. The DLM Client for the Moxa DLM Service now implements a back-off 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 back off mode, progressively increasing the message delay up to a maximum of 60 minutes.
 - During back off, events are sent as compressed messages with an indication of suppression count (e.g., "backed off for x times").
 - Normal message delivery resumes when the event stops occurring or after a device reboot.

Fixed Issues

1. When the WAN connection was restored by replugging the Ethernet cable, the connection to the AWS IoT Core service was not re-established.
2. The certificate wasn't received properly after the AIG was fully registered, and the Moxa DLM Service returned error code 500.

3. 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.
4. Upgrading thingspro-agent to v2.3.0 extended the Azure IoT Edge module token refresh interval to reduce disconnection risks.
5. Failed to establish a 2G cellular connection in the EU.
6. The DO value didn't refresh immediately when the tag value had been modified.
7. The refresh button on IO did not update info.

Changes

7. Upgrade Azure IoT Device SDK to LTS_03_2025.
8. 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.
9. Sensitive and confidential data under the ThingsPro folder is now protected by permission control. Unauthorized users cannot read, write, or execute such data.
10. OPC UA Server changes:
 - The OPC UA server now generates X.509 private keys with a length of 2048 bits.
 - The signing algorithm has been upgraded to SHA-256.
 - Existing OPC UA server certificates will continue to be used. The new key length and algorithm apply only to certificates generated after the v1.8.0 upgrade.
 - The OPC UA server no longer includes any default or built-in user accounts.
 - User account information is now excluded from the OPC UA server's configuration import/export operations.
11. The Wi-Fi AP feature no longer ships with a default password.
12. Function changes:
 - The Function (container) has been upgraded from Python 3.9 to Python 3.10.8
 - For Python package migration, the system will automatically reinstall the user's desired packages with network access; or you can call GET /api/v1/function/requirements/migration to retrieve the list of desired packages without network access. To provide flexibility, new APIs are available to manage the migration process:
 - i. **GET /api/v1/function/requirements/migration:** Fetch current settings, migration results, and desired packages.
 - ii. **PUT /api/v1/function/requirements/migration:** Update settings (e.g., enable/disable migration, timeout duration).

Notes

1. Tag dashboard value precision issue
The tag monitor may display incorrect values when handling numbers beyond JavaScript's safe

integer range ($\pm 2^{53} - 1$, i.e., from -9,007,199,254,740,991 to 9,007,199,254,740,991).

This is because of 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.

2. Upgrading from the local drive to upload the upgrade package requires a minimum upload speed of 1MB/sec.
3. The OPC UA Server certificate generation may rarely fail because of a race condition, which may be triggered if the apply operation is executed immediately after the regeneration operation in very quick succession. Perform an enable/disable OPC UA Server cycle to restore normal operations.
4. The upgrade process from firmware v1.4.0 to v1.5.0 requires approximately 20+ minutes.

Which products will be affected?

Product Name	Current Version	New Version
AIG-101 Series	V1.2.0	V1.3.0
AIG-301 Series	V1.7.0	V1.8.0
AIG-501 Series	V1.4.0	V1.5.0

When will the new versions be available?

Product Name	New Version	Available for Order
AIG-101 Series	V1.3.0	Available Now
AIG-301 Series	V1.8.0	Available Now
AIG-501 Series	V1.5.0	Available Now

If you have any questions, please contact alfredfh.li@moxa.com, or contact your regional sales representative.