Getting Started Guide

For AWS IoT Core Integration

GoodLinker IIoT Gateway
BCS-MX Edge Computer

Edition 1.0.0, February 2026

GoodLinker BCS-MX AWS IoT Core Getting Started Guide (Vendor-Managed Mode)

1. Introduction

1.1 Purpose of This Guide

This document provides a step-by-step guide for getting started with the GoodLinker BCS-MX IIoT Gateway when used with AWS IoT Core in a vendor-managed integration model.

The purpose of this guide is to help users understand how the BCS-MX establishes a secure connection to AWS IoT Core, how cloud connectivity is enabled from the device, and how to verify successful data transmission to the cloud.

This guide focuses on the initial cloud enablement and connectivity verification process, rather than detailed device configuration or application-specific usage.

1.2 Supported Device

This guide applies to the following device model:

- Product Name: GoodLinker IIoT Gateway
- Model: BCS-MX

The BCS-MX is an industrial data acquisition gateway designed for OT/IIoT environments. It collects data from industrial equipment and systems (such as PLCs, sensors, meters, and controllers) and securely transmits structured telemetry to cloud services via AWS IoT Core.

1.3 AWS IoT Core Integration Model

The BCS-MX uses a vendor-managed AWS IoT Core integration model.

In this model:

- AWS IoT Core connectivity, certificates, IoT policies, and endpoints are pre-configured and managed by GoodLinker.
- End users are not required to create or manage AWS IoT Core resources, such as Things, certificates, or policies.
- Users enable or disable cloud data publishing directly from the BCS-MX device interface.

This approach simplifies deployment while maintaining secure, TLS-based communication with AWS IoT Core.

1.4 Scope and Assumptions

This guide assumes that:

- The BCS-MX device has been physically installed and powered on.
- Basic local device setup has been completed.
- The device has access to the internet.

Detailed instructions for physical installation, wiring, and advanced device configuration are outside the scope of this guide and are documented separately in the GoodLinker BCS-MX Quick Installation Guide and User Manual.

1.5 Audience

This guide is intended for:

- System integrators and solution partners deploying the BCS-MX
- Technical users responsible for enabling cloud connectivity
- AWS reviewers and partners evaluating AWS IoT Core–based device integrations

2. AWS IoT Core Integration Overview

2.1 Integration Model Overview

The GoodLinker BCS-MX integrates with AWS IoT Core using a vendor-managed deployment model.

In this model, AWS IoT Core serves as the secure cloud connectivity layer for device-to-cloud communication. All AWS IoT Core–related resources, including device provisioning, certificates, IoT policies, and endpoints, are managed and maintained by GoodLinker as part of the platform service.

End users interact with AWS IoT Core indirectly through the BCS-MX device interface and are not required to configure or manage AWS resources themselves.

2.2 Responsibilities and Security Boundaries

The responsibilities within the vendor-managed integration model are clearly defined as follows:

Managed by GoodLinker

- AWS IoT Core device provisioning
- X.509 certificates and key lifecycle management
- IoT policies and topic permissions
- Secure MQTT over TLS communication
- Cloud connectivity retry and reconnection mechanisms

Managed by the User Environment

- Physical installation of the device
- Network connectivity and internet access
- Firewall rules allowing outbound TLS connections
- Local data source configuration (e.g., Modbus devices, sensors, controllers)

This separation of responsibilities ensures secure operation while minimizing deployment complexity for end users.

2.3 Security and Communication Model

The BCS-MX communicates with AWS IoT Core using MQTT over TLS.

All device-to-cloud communication is encrypted using TLS, and authentication is performed using device-specific credentials managed by GoodLinker. The device continuously monitors its cloud connection state and automatically attempts reconnection in the event of network interruptions.

This design provides secure and reliable data transmission suitable for industrial environments where network stability may vary.

2.4 Role of AWS IoT Core in the Solution

Within the overall solution architecture, AWS IoT Core functions as the secure message ingestion and device connectivity layer.

AWS IoT Core is responsible for:

- Authenticating the device
- Receiving telemetry data published by the BCS-MX
- Providing a scalable and reliable cloud entry point for device data

The data received by AWS IoT Core is then processed and utilized by the GoodLinker Cloud of War Room platform for monitoring, visualization, and further analysis.

AWS IoT Core is not bypassed or replaced by private cloud components and remains an integral part of the solution's cloud architecture.

2.5 User Interaction with Cloud Connectivity

Users enable or disable cloud connectivity directly on the BCS-MX device through the device management interface.

When cloud connectivity is enabled:

- **The device establishes a secure connection to AWS IoT Core**
- **Telemetry data collected from local data sources is published to predefined cloud topics**
- **Cloud connection status and data transmission indicators are updated in the device interface**

This interaction model allows users to control cloud data publishing without requiring direct access to AWS IoT Core services.

3. Solution Architecture

3.1 Architectural Overview

The GoodLinker BCS-MX is designed as an industrial edge gateway that connects operational technology (OT) environments to cloud services in a secure and structured manner.

The overall solution architecture follows a clear, layered model:

- **Industrial Field Layer – Data sources such as PLCs, sensors, meters, and controllers**
- **Edge Gateway Layer – Data acquisition, normalization, and cloud control performed by the BCS-MX**
- **Cloud Connectivity Layer – Secure device-to-cloud communication provided by AWS IoT Core**
- **Application Layer – Cloud-based monitoring and management services**

This architecture ensures that all device-originated data is transmitted through AWS IoT Core as the standardized cloud ingress point.

3.2 Industrial Field and Edge Integration

At the industrial field level, the BCS-MX connects to a wide range of equipment using standard industrial interfaces and protocols.

The edge gateway is responsible for:

- **Communicating with industrial devices using supported protocols**
- **Collecting raw operational data from connected equipment**
- **Structuring and organizing data into defined telemetry models**
- **Preparing data for secure transmission to the cloud**

By performing these tasks at the edge, the BCS-MX minimizes cloud-side complexity and reduces the need for direct cloud integration at the device level.

3.3 Device-to-Cloud Data Flow

When cloud connectivity is enabled, the data flow proceeds as follows:

- **The BCS-MX collects and processes data from configured industrial data sources.**
- **Structured telemetry data is published by the BCS-MX to AWS IoT Core using MQTT over TLS.**
- **AWS IoT Core authenticates the device and receives incoming messages as the secure cloud entry point.**

- Cloud applications consume the data received through AWS IoT Core for further processing and visualization.

This flow ensures a consistent and secure device-to-cloud communication path suitable for large-scale industrial deployments.

3.4 Role of AWS IoT Core

AWS IoT Core functions as the central device connectivity and message ingestion service within the solution architecture.

Specifically, AWS IoT Core is responsible for:

- Secure device authentication
- TLS termination for device connections
- Receiving and handling MQTT telemetry messages
- Providing a scalable and highly available cloud connectivity layer

AWS IoT Core is a required and integral component of the architecture and is not bypassed or replaced by private messaging systems.

3.5 Role of the Application Layer

The GoodLinker Cloud of War Room platform represents the application layer of the solution.

After telemetry data is ingested through AWS IoT Core, the application layer provides:

- Monitoring and visualization of device and operational data
- Aggregated views across multiple devices or sites
- Operational insights derived from collected telemetry

The application layer does not establish direct connections to edge devices. All device-originated data is delivered through AWS IoT Core, maintaining a clear separation between connectivity and application logic.

3.6 Architectural Characteristics

Key characteristics of the solution architecture include:

- AWS-centric connectivity – AWS IoT Core is the sole cloud ingress for device data
- Edge-controlled data flow – Cloud publishing is explicitly controlled at the device level
- Secure communication – All device-to-cloud communication uses encrypted channels
- Scalable deployment model – The architecture supports large numbers of deployed devices
- Industrial resilience – Edge processing and buffering support operation in variable network conditions

These characteristics make the architecture suitable for industrial and OT environments that require reliable, secure, and scalable cloud integration.

4. Prerequisites

Before enabling AWS IoT Core connectivity on the BCS-MX, ensure that the following prerequisites are met.

4.1 Device Requirements

- A supported GoodLinker BCS-MX IIoT Gateway
- The device is powered on and has completed the initial boot process
- Basic local device setup has been completed

Detailed instructions for physical installation and initial setup are provided in the GoodLinker BCS-MX Quick Installation Guide.

4.2 Network Requirements

- An active internet connection is available to the device
- Outbound network access is permitted for secure TLS communication
- Firewall rules allow outbound connections required for cloud communication

No inbound ports or port forwarding are required for AWS IoT Core connectivity.

4.3 Time Synchronization

- The device system time must be correctly synchronized

Accurate system time is required to establish secure TLS connections. Time synchronization is handled automatically by the device when network access is available.

4.4 Data Source Configuration

- At least one local data source (such as a PLC, sensor, meter, or controller) has been configured on the BCS-MX
- Data polling or collection is functioning correctly at the local level

Cloud data publishing can only occur when valid data is available from configured local sources.

4.5 AWS Account Requirement

- No AWS account is required for end users

All AWS IoT Core resources required for device connectivity are provisioned and managed by GoodLinker as part of the vendor-managed integration model.

5. Device Setup

5.1 Purpose of This Section

This section provides a high-level reference for the local device setup required before enabling AWS IoT Core connectivity.

It does not replace the full installation or configuration documentation. Instead, it summarizes the minimum local setup conditions that must be completed to ensure successful cloud enablement.

5.2 Physical Installation and Power-Up

Before configuring cloud connectivity, ensure that the BCS-MX has been:

- Physically installed according to the recommended mounting and wiring guidelines
- Properly powered on
- Allowed to complete the initial system boot process

Detailed physical installation instructions, including mounting, wiring, and power specifications, are documented in the GoodLinker BCS-MX Quick Installation Guide.

5.3 Local Access and Initial Configuration

Local access to the BCS-MX is required to perform initial configuration tasks.

At a minimum, the following must be completed:

- Access the device management interface (Web UI)
- Configure basic system settings
- Verify that the device is operating normally

Authentication and interface details are documented in the GoodLinker BCS-MX User Manual.

5.4 Data Source Configuration

Before enabling cloud data publishing, at least one valid data source must be configured on the device.

This typically includes:

- Defining communication parameters for connected industrial devices
- Verifying that data polling or data acquisition is functioning correctly
- Confirming that collected data is visible in the local device interface

Cloud publishing depends on valid local data and will not function if no data sources are configured.

5.5 Readiness Checklist

Before proceeding to cloud enablement, confirm that:

- The device is powered on and reachable
- Local configuration is complete
- At least one data source is actively providing data
- Network connectivity is available

Once these conditions are met, the device is ready for AWS IoT Core cloud enablement.

6. Enabling AWS IoT Core Cloud Upload

6.1 Overview

The BCS-MX allows users to enable or disable cloud data publishing directly from the device management interface.

Enabling cloud upload activates the device’s vendor-managed AWS IoT Core connectivity, allowing telemetry data collected at the edge to be securely published to the cloud.

No manual AWS configuration is required during this process.

6.2 Accessing the Device Management Interface

To enable cloud upload, access the BCS-MX device management interface:

- Connect to the BCS-MX through the local network.
- Log in to the device Web UI using authorized credentials.
- Navigate to the cloud or system configuration section of the interface.

Authentication and access details are documented in the GoodLinker BCS-MX User Manual.

6.3 Enabling Cloud Upload

After local setup and data source configuration are complete, enable cloud upload as follows:

- Locate the Cloud Upload or Cloud Connectivity setting in the device interface.
- Set the cloud upload switch to the Enabled state.

- Save or apply the configuration changes.

When cloud upload is enabled, the BCS-MX initiates a secure connection to AWS IoT Core and begins publishing telemetry data according to the configured data model.

6.4 System Behavior After Enabling Cloud Upload

Once cloud upload is enabled, the following behavior is expected:

- The device establishes a secure MQTT over TLS connection to AWS IoT Core.
- Device authentication is performed using vendor-managed credentials.
- Telemetry data from configured data sources is published to predefined cloud topics.
- The device continuously monitors connection status and automatically attempts reconnection if the connection is interrupted.

Initial connection and data publishing may take a short period to complete, depending on network conditions.

6.5 Disabling Cloud Upload

Cloud upload can be disabled at any time from the device interface.

When cloud upload is disabled:

- The connection to AWS IoT Core is terminated.
- No new telemetry data is published to the cloud.
- Local data collection and device operation continue unaffected.

This allows users to control when data is transmitted to the cloud without modifying AWS-side configurations.

6.6 Configuration Persistence

The cloud upload setting is retained across device restarts.

If the device is rebooted while cloud upload is enabled, it will automatically attempt to re-establish the AWS IoT Core connection once network connectivity is available.

7. Verifying AWS IoT Core Connectivity

7.1 Verification Model

The GoodLinker BCS-MX operates in a vendor-managed connectivity model, where AWS IoT Core credentials and cloud configuration are pre-provisioned by the vendor.

As a result, end users are not required to manually create AWS IoT resources or access the AWS Management Console in order to verify connectivity.

Connectivity verification is performed through device-level status indicators and application-level confirmation, as described below.

7.2 Device-Level Connection Status

Once cloud upload is enabled on the BCS-MX, the device automatically attempts to establish a secure MQTT connection to AWS IoT Core.

The device provides a connection status indicator within its local management interface to reflect the current cloud connectivity state.

A successful connection is indicated by:

- Cloud connection status shown as *Connected*
- No active error or retry messages related to cloud communication
- Continuous operation without manual intervention

If the device is unable to connect, the status indicator reflects a disconnected or retrying state, allowing users to identify connectivity issues at the device level.

7.3 Cloud-Side Confirmation via Application Layer

After a successful connection to AWS IoT Core, telemetry data published by the BCS-MX becomes available to cloud applications subscribed to the corresponding AWS IoT topics.

Connectivity can be confirmed by observing:

- Incoming telemetry data visible in the cloud application dashboard
- Timestamped data updates corresponding to the configured publish interval
- Consistent data flow without interruption

Because all device-originated data is routed through AWS IoT Core, successful data visibility at the application layer implicitly confirms successful AWS IoT Core connectivity.

7.4 Transport and Security Characteristics

The BCS-MX connects to AWS IoT Core using the following transport and security mechanisms:

- MQTT protocol over TLS encryption
- Device authentication using X.509 certificates
- Automatic reconnection handling for transient network interruptions

These mechanisms ensure secure and reliable communication between the device and AWS IoT Core without requiring user intervention.

7.5 No Direct AWS Console Access Required

In this solution, verification of AWS IoT Core connectivity does not require:

- Access to the AWS Management Console
- Manual inspection of AWS IoT Things, policies, or certificates
- Direct interaction with AWS IoT Core topics by end users

This approach is intentional and aligns with the vendor-managed deployment model commonly used in industrial environments, where cloud infrastructure is centrally managed and abstracted from end users.

7.6 Summary

AWS IoT Core connectivity for the GoodLinker BCS-MX can be verified through a combination of:

- Device-level connection status indicators
- Application-level confirmation of incoming telemetry data

Together, these methods provide clear evidence of successful and secure communication with AWS IoT Core while maintaining a simplified user experience and protecting cloud configuration details.

8. Troubleshooting

This section describes common scenarios related to AWS IoT Core connectivity and provides guidance for identifying and resolving issues.

8.1 Device Does Not Connect to AWS IoT Core

Possible causes:

- Network connectivity is unavailable or unstable
- Required outbound ports are blocked by firewall rules
- DNS resolution is not available on the network

Recommended checks:

- Verify that the device has a valid IP address and can access the internet
- Ensure outbound traffic over TCP port 8883 is allowed
- Confirm that DNS resolution is functioning correctly

8.2 Cloud Connection Status Remains Disconnected

Possible causes:

- Temporary network interruption
- Incorrect system time on the device
- TLS handshake failure due to network restrictions

Recommended checks:

- Wait for automatic reconnection to complete
- Verify that the system time is synchronized correctly
- Review local status indicators for retry or error messages

The BCS-MX automatically retries cloud connections without requiring manual intervention.

8.3 Data Not Appearing in Cloud Application

Possible causes:

- Cloud upload is not enabled for the selected data group
- No active data source is configured
- Publish interval has not yet elapsed

Recommended checks:

- Confirm that cloud upload is enabled in the device configuration
- Verify that at least one data source is correctly configured
- Allow sufficient time for the first publish cycle to complete

8.4 Intermittent Data Upload

Possible causes:

- Unstable network connectivity
- Temporary loss of internet access

Recommended checks:

- Monitor network stability at the deployment site
- Confirm that connectivity is restored after interruptions

The device is designed to handle transient network conditions and resume data upload automatically when connectivity is restored.

8.5 When to Contact Support

If issues persist after performing the recommended checks:

- Collect basic device information (device ID, firmware version)
- Capture relevant status messages from the local interface
- Contact GoodLinker support for further assistance

8.6 Summary

Most connectivity-related issues can be resolved by verifying basic network conditions and device configuration.

The BCS-MX is designed to automatically manage cloud connectivity and recover from temporary network interruptions, minimizing the need for manual troubleshooting.

The GoodLinker Cloud of War Room Platform

The BCS-MX integrates with the GoodLinker “Cloud of War Room” IIoT service to support industrial equipment monitoring, structured telemetry visualization, and remote operational supervision. Through this cloud service, data collected by the gateway can be synchronized to dashboards for production status display, equipment condition monitoring, ESG indicator review, and anomaly notifications.

Users may view real-time telemetry, trend charts, and machine status via the web console or mobile app. This service helps transform traditional equipment into IoT-ready assets by providing digital visibility and standardized data interfaces on top of existing industrial infrastructure.

Web Dashboard: https://warroom.goodlinker.io/

Mobile App – iOS: https://apps.apple.com/tw/app/goodlinker/id1476501530?l=en

Mobile App – Android: https://play.google.com/store/apps/details?id=com.goodlinker.mobile

History of Specification

Edition	Date / Released	Changed
1.0.0	2026/02/02	New release

If any performance specifications, firmware behavior, interface configurations, or functional characteristics of this device are modified, this document must be updated in real time to ensure all information remains accurate and aligned with the current product release.

Manufacturer Information

Name of Company: GoodLinker Co., LTD

Official Website: https://www.goodlinker.io/

Product Information: https://www.goodlinker.io/product/BCS-MX

Address: Ltd. No. 40, Section 3, Zhongshan North Road, Zhongshan District, Taipei City 104327, Taiwan (R.O.C)

Email: info@goodlinker.io

Telephone: +886-2-25997987