Airlinq® Online Technical specifications

This document is intended for IT administrators or technical staff responsible for establishing connection from one or more Airmaster Air Handling Units (AHU in the following) to the Airlinq® Online cloud service.

Overview

Airlinq® Online is an online Cloud Service consisting of a Device Gateway Server and a Web App.
The Cloud Service is hosted by Microsoft Azure (West Europe).
The Cloud Service handles all AHUs across customers and projects. Access is restricted by user authentication.
All access and communication is encrypted per default (see the encryption section below).

We advise connecting the AHUs to a dedicated internal IoT network, ensuring separation from the network used by office PCs and other devices. This separation is essential to maintain network integrity and efficiency, reducing the risk of interference, security vulnerabilities, and potential performance issues between the AHUs and standard office equipment.

Device gateway server

Airlinq L and P control box

The Device Gateway Server handles communication with each AHU.
Each AHU is pre-programmed to communicate with a certain gateway address when an Internet connection is established through the built-in Ethernet module. Subsequently the AHU communicates its status to the same gateway in certain intervals.

Communication is always initiated by the AHUs and no ports need to be opened for inbound communication to the AHUs.
The AHU acts as a TCP Client and connect to the Device Gateway Servers on port 55556. DNS: gateway.airlinq.eu.

Normally, once the AHU has established the connection, the communication is free to flow both ways until the session is over and is not limited by firewalls. However, some organisations have very strict firewall policies and will not allow any reply from the Device Gateway Server.
In such cases a firewall rule/exception must be added by the customer for the Airlinq® Online Cloud Service to work.

During the commissioning phase UDP communication is used for AHU device discovery on the internal network.
This is not required to be supported on the network, but it will ease the work for the technicians during the commissioning.

Airlinq Aware control box (AMX 4)

The Azure IoT Hub handles communication with each AHU.

Azure IoT Hub ensures secure communication between AHU and the cloud through several mechanisms, including the use of shared access tokens and the MQTT protocol.

Each device communicates securely with the IoT Hub using **Shared Access Signatures (SAS tokens).** The SAS token is included in the MQTT protocol's authentication headers. This ensures that only authorized devices with a valid token can establish a connection to the IoT Hub.

Azure IoT Hub enforces **TLS (Transport Layer Security)** encryption on all MQTT connections. This ensures that data transmitted between devices and the cloud is encrypted and protected from interception or tampering. The TCP traffic connects to the servers on port 8883. DNS: iot-airlinq-airmaster-prod-1.azure-devices.net.

Web App

The Web App is accessible through https://online.airlinq.eu and acts as portal that enables users to access and monitor one or more Airmaster AHUs. The Web App is designed with the principles of responsive web design in mind making it compatible with almost any device form factor and operating system.

IP Address

Airling L and P control box
Per default the AHU requests a dynamic IP address from a DHCP server.
It is possible to set a static IP address on each AHU using the Airlinq Service Tool PC software.

Airling Aware control box (AMX 4)
Per default the AHU requests a dynamic IP address from a DHCP server.

Encryption

Airling L and P control box
Encryption is used throughout the system – both between AHUs and the Device Gateway and between end users and the Web App.
The AHU communicates with the Device Gateway Server using a proprietary binary protocol which uses an AES128 encryption with a unique key per AHU.
SSL encryption is used between end users and the Web App (HTTPS).

Airling Aware control box (AMX 4)
Azure IoT Hub enforces **TLS (Transport Layer Security)** encryption on all MQTT connections. This ensures that data transmitted between devices and the cloud is encrypted and protected from interception or tampering.

Communication

Airling L and P control box
The AHU uses half-duplex communication. It is required that the switches for the AHUs can handle half-duplex communication.

The AHU can only communicate at a network of 250 Mbit or lower, if there is a higher speed on the location a switch can be used with half-duplex and Auto-Negotiation.

Airling Aware control box (AMX 4)
The AHU uses full-duplex communication.