

Airlinq® Online Technische specificaties

Dit document is bedoeld voor IT-beheerders en technisch personeel dat verantwoordelijk is voor het tot stand brengen van een verbinding tussen een of meer Airmaster Air Handling Units (hierna AHU, ventilatie-units) en de Airlinq® Online-cloudservice.

Overzicht

Airlinq® Online is een online clouddienst die bestaat uit een Device Gateway Server en een webapp.

De clouddienst wordt gehost door Microsoft Azure (West-Europa).

De clouddienst beheert alle AHU's van klanten en projecten. Toegang wordt beveiligd door gebruikersauthenticatie.

Alle toegang en communicatie worden standaard gecodeerd (zie het gedeelte over encryptie hieronder).

Wij adviseren om de AHU's aan te sluiten op een speciaal intern IoT-netwerk, zodat ze gescheiden zijn van het netwerk dat wordt gebruikt door kantoor-pc's en andere apparaten. Deze scheiding is essentieel om de integriteit en efficiëntie van het netwerk te behouden en om het risico op interferentie, beveiligingsproblemen en mogelijke prestatieproblemen tussen de AHU's en standaard kantoorapparatuur te verminderen.

Device Gateway Server

Airlinq L en P mainbox

De Device Gateway Server verzorgt de communicatie met elke AHU.

Elke AHU is voorgeprogrammeerd om te communiceren met een bepaald gateway-adres wanneer er een internetverbinding tot stand wordt gebracht via de ingebouwde Ethernet-module. Vervolgens communiceert de AHU op vaste tijdstippen zijn status naar dezelfde gateway.

De communicatie wordt altijd geïnitieerd door de AHU's, er hoeven geen poorten te worden geopend voor inkomende communicatie met de AHU's.

De AHU fungeert als een TCP-client en maakt verbinding met de Device Gateway-servers op poort 55556. DNS: gateway.airlinq.eu.

Zodra de AHU de verbinding heeft gemaakt, kan de communicatie normaal gesproken vrij in beide richtingen verlopen totdat de sessie voorbij is, zonder beperkingen door firewalls. Sommige organisaties hanteren echter een zeer strikt firewallbeleid en staan geen enkel antwoord van de Device Gateway Server toe.

In dergelijke gevallen moet de klant een firewallregel of uitzondering toevoegen om de Airlinq® Online Cloud Service te laten werken.

Tijdens de inbedrijfstellingsfase wordt UDP-communicatie gebruikt voor de detectie van AHU-apparaten op het interne netwerk. Dit hoeft niet per se op het netwerk te worden ondersteund, maar het vereenvoudigt wel het werk voor de technici tijdens de inbedrijfstelling.

Airlinq Aware mainbox (AMX 4)

De Azure IoT Hub verzorgt de communicatie met elke AHU.

Azure IoT Hub zorgt voor veilige communicatie tussen AHU en de cloud via verschillende mechanismen, waaronder het gebruik van gedeelde toegangstokens en het MQTT-protocol.

Elk apparaat communiceert veilig met de IoT Hub met behulp van **Shared Access Signatures (SAS-tokens)**. Het SAS-token is opgenomen in de authenticatieheaders van het MQTT-protocol. Dit zorgt ervoor dat alleen geautoriseerde apparaten met een geldig token verbinding kunnen maken met de IoT Hub.

Azure IoT Hub dwingt **TLS (Transport Layer Security)**-encryptie af op alle MQTT-verbindingen. Hiermee wordt gegarandeerd dat gegevens die tussen apparaten en de cloud worden verzonden, worden gecodeerd en beschermd tegen onderschepping of manipulatie. Het TCP-verkeer maakt verbinding met de servers op poort 8883. DNS: iot-airlinq-airmaster-prod-1.azure-devices.net

Webapp

De webapp is toegankelijk via <https://online.airling.eu> en fungeert als portaal waarmee gebruikers toegang kunnen krijgen tot een of meer Airmaster AHU's en deze kunnen bewaken. De webapp is ontworpen volgens de principes van responsief webdesign, waardoor deze compatibel is met vrijwel elk apparaat en besturingssysteem.

IP-adres

Airling L en P mainbox

De AHU vraagt standaard een dynamisch IP-adres aan bij een DHCP-server.

Het is mogelijk om op elke AHU een statisch IP-adres in te stellen met behulp van de Airling Service Tool pc-software.

Airling Aware mainbox (AMX 4)

De AHU vraagt standaard een dynamisch IP-adres aan bij een DHCP-server.

Encryptie

Airling L en P mainbox

In het hele systeem wordt gebruikgemaakt van encryptie, zowel tussen AHU's en de Device Gateway als tussen eindgebruikers en de webapp.

De AHU communiceert met de Device Gateway Server via een propriëtair binair protocol dat gebruikmaakt van AES128-encryptie met een unieke sleutel per AHU.

SSL-encryptie wordt gebruikt tussen eindgebruikers en de webapp (HTTPS).

Airling Aware mainbox (AMX 4)

Azure IoT Hub dwingt **TLS (Transport Layer Security)**-encryptie af op alle MQTT-verbindingen. Hiermee wordt gegarandeerd dat gegevens die tussen apparaten en de cloud worden verzonden, worden gecodeerd en beschermd tegen onderschepping of manipulatie.

Communicatie

Airling L en P mainbox

De AHU maakt gebruik van half-duplexcommunicatie. Het is vereist dat de switches voor de AHU's half-duplexcommunicatie aankunnen.

De AHU kan alleen communiceren op een netwerk van 250 Mbit of lager. Als er op de locatie een hogere snelheid wordt gebruikt, kan een switch met half-duplex en Auto-Negotiation worden gebruikt.

Airling Aware mainbox (AMX 4)

De AHU maakt gebruik van full-duplexcommunicatie.