

Airlinq® Online Tekniske specifikationer

Dette dokument henvender sig til IT-administratorer eller teknisk personale, der er ansvarlige for at etablere forbindelse fra en eller flere Airmaster Air Handling Units (herefter: AHU) til Airlinq® Online cloud-tjenesten.

Oversigt

Airlinq® Online er en online cloud-tjeneste, der består af en Device Gateway-server og en web-app.

Cloud-tjenesten hostes af Microsoft Azure (Vesteuropa).

Cloud-tjenesten håndterer alle AHU'er på tværs af kunder og projekter. Adgang er begrænset af brugergodkendelse.

AI adgang og kommunikation er som standard krypteret (se krypteringsafsnittet nedenfor).

Vi anbefaler at tilslutte AHU'erne til et dedikeret internt IoT-netværk for at sikre adskillelse fra det netværk, der bruges af kontor-pc'er og andre enheder. Denne adskillelse er afgørende for at opretholde netværkets integritet og effektivitet, idet det reducerer risikoen for interferens, sikkerhedssårbarheder og potentielle ydeevneproblemer mellem AHU'erne og standardkontorudstyr.

Device Gateway-server

Airlinq L- og P-kontrolboks

Device Gateway-serveren håndterer kommunikationen med hver enkelt AHU.

Hver AHU er indstillet til at kommunikere med en bestemt gateway-adresse, når en internetforbindelse oprettes via det indbyggede Ethernet-modul. Derefter kommunikerer AHU'en sin status til den samme gateway i bestemte intervaller.

Kommunikation initieres altid af AHU'erne, og det er ikke nødvendigt at åbne porte for indgående kommunikation til AHU'erne.

AHU'en fungerer som en TCP-klient og opretter forbindelse til Device Gateway-serverne på port 55556. DNS: gateway.airlinq.eu.

Normalt er kommunikationen fri til at strømme begge veje, når AHU'en har etableret forbindelsen, indtil sessionen er afsluttet, og den begrænses ikke af firewalls. Nogle virksomheder har imidlertid meget strenge firewall-politikker og vil ikke tillade nogen svar fra Device Gateway-serveren.

I sådanne tilfælde skal kunden tilføje en firewall-regel eller -undtagelse, for at Airlinq® Online Cloud-tjenesten kan fungere.

I idriftsættelsesfasen bruges UDP-kommunikation til at registrere AHU-enheder på det interne netværk. Det er ikke nødvendigt, at dette understøttes af netværket, men det vil lette arbejdet for teknikerne under idriftsættelsen

Airlinq Aware-kontrolboks (AMX 4)

Azure IoT-hubben står for kommunikationen med hver enkelt AHU.

Azure IoT-hubben sikrer sikker kommunikation mellem AHU og skyen ved hjælp af flere mekanismer, herunder brugen af delte adgangstokens og MQTT-protokollen.

Hver enhed kommunikerer sikkert med IoT-hubben ved hjælp af **Shared Access Signatures (SAS-tokens)**. SAS-tokenet er inkluderet i MQTT-protokollens autentificeringsoverskrifter. Dette sikrer, at kun autoriserede enheder med et gyldigt token kan oprette forbindelse til IoT-hubben.

Azure IoT-hubben gennemtvinger **TLS (Transport Layer Security)**-kryptering på alle MQTT-forbindelser. Dette sikrer, at data sendt mellem enheder og skyen er krypteret og beskyttet mod aflytning eller manipulation. TCP-trafikken forbinder til serverne på port 8883. DNS: iot-airlinq-airmaster-prod-1.azure-devices.net.

Web-app

Web-appen er tilgængelig via <https://online.airlinq.eu> og fungerer som en portal, der gør det muligt for brugere at få adgang til at overvåge en eller flere Airmaster AHU'er. Web-appen er designet med fokus på principperne for responsivt webdesign, hvilket gør den kompatibel med næsten enhver enhedstype og ethvert operativsystem.

IP-adresse

[Airlinq L- og P-kontrolboks](#)

Som standard anmoder AHU'en om en dynamisk IP-adresse fra en DHCP-server.

Det er muligt at indstille en statisk IP-adresse på hver AHU ved hjælp af Airlinq Service Tool PC-softwaren.

[Airlinq Aware-kontrolboks \(AMX 4\)](#)

Som standard anmoder AHU'en om en dynamisk IP-adresse fra en DHCP-server.

Kryptering

[Airlinq L- og P-kontrolboks](#)

Kryptering bruges overalt i systemet – både mellem AHU'er og Device Gateway og mellem slutbrugere og web-appen.

AHU'en kommunikerer med Device Gateway-serveren ved hjælp af en proprietær binær protokol, som bruger AES128-kryptering med en unik nøgle pr. AHU.

SSL-kryptering bruges mellem slutbrugere og web-appen (HTTPS).

[Airlinq Aware-kontrolboks \(AMX 4\)](#)

Azure IoT-hubben gennemtvinger **TLS (Transport Layer Security)**-kryptering på alle MQTT-forbindelser. Dette sikrer, at data sendt mellem enheder og skyen er krypteret og beskyttet mod aflytning eller manipulation.

Kommunikation

[Airlinq L- og P-kontrolboks](#)

AHU'en bruger halv-duplex-kommunikation. Det er nødvendigt, at switchene til AHU'erne kan håndtere halv-duplex-kommunikation.

AHU'en kan kun kommunikere på et netværk, der er på 250 Mbit eller derunder. Hvis der benyttes en højere hastighed på stedet, kan en switch bruges med halv-duplex og Auto-Negotiation.

[Airlinq Aware-kontrolboks \(AMX 4\)](#)

AHU'en bruger fuld-duplex-kommunikation.