Airlinq® Online Technische Daten

Diese Unterlage ist für IT-Administratoren oder technisches Personal vorgesehen, die eine Verbindung von einem oder mehreren Airmaster-Lüftungsgeräten zum Airlinq®-Online-Cloud-Dienst herstellen sollen.

Überblick

Airlinq® Online ist ein Online-Cloud-Dienst mit einem Geräte-Gateway-Server und einer Web-App.
Der Cloud-Dienst wird von Microsoft Azure (Westeuropa) gehostet.
Der Cloud-Dienst verwaltet alle Lüftungsgeräte kunden- und projektübergreifend. Der Zugriff ist nur angemeldeten Benutzern möglich.
Alle Zugriffe und Kommunikationen sind standardmäßig verschlüsselt (siehe unten im Abschnitt zur Verschlüsselung).

Wir empfehlen, die Lüftungsgeräte an ein eigenes, internes IoT-Netzwerk anzuschließen, getrennt vom Netzwerk für Bürocomputer und andere Geräte. Diese Trennung ist wichtig für die Netzwerkintegrität und den Wirkungsgrad und um das Risiko von Störungen, Sicherheitslücken und möglichen Leistungsproblemen zwischen den Lüftungsgeräten und gängigen Bürogeräten zu verringern.

Geräte-Gateway-Server

Airlinq L- und P-Steuerbox

Der Geräte-Gateway-Server übernimmt die Kommunikation mit jedem Lüftungsgerät.
Jedes Lüftungsgerät ist so vorprogrammiert, dass es mit einer bestimmten Gateway-Adresse kommuniziert, wenn über das integrierte Ethernet-Modul eine Internetverbindung hergestellt wird. Anschließend übermittelt das Lüftungsgerät in bestimmten Zeitabständen seinen Zustand an dasselbe Gateway.

Die Kommunikation wird immer von den Lüftungsgeräten eingeleitet und es müssen keine Schnittstellen für eingehende Kommunikation mit den Lüftungsgeräten geöffnet werden.
Das Lüftungsgerät fungiert als TCP-Client und stellt über Anschluss 55556 eine Verbindung zu den Geräte-Gateway-Servern her.
DNS: gateway.airlinq.eu.

Wenn das Lüftungsgerät die Verbindung hergestellt hat, kann die Kommunikation in der Regel bis zum Sitzungsende in beide Richtungen frei und ohne Einschränkungen durch Firewalls fließen. Manche Unternehmen haben jedoch sehr strenge Firewall-Vorschriften und lassen keine Antworten vom Geräte-Gateway-Server zu.
In solchen Fällen muss der Kunde eine Firewall-Regel oder -Ausnahme einrichten, damit der Airlinq® Online-Cloud-Dienst funktioniert.

Während der Inbetriebnahme wird die UDP-Kommunikation zur Lüftungsgeräteerkennung im internen Netzwerk verwendet. Diese muss zwar nicht zwingend im Netzwerk unterstützt werden, erleichtert den Technikern aber die Inbetriebnahme.

Airlinq Aware-Steuerbox (AMX 4)

Der Azure IoT Hub übernimmt die Kommunikation mit den Lüftungsgeräten.

Mithilfe mehrerer Mechanismen sichert der Azure IoT Hub die Kommunikation zwischen Lüftungsgerät und der Cloud, darunter die Verwendung gemeinsamer Zugriffstoken und des MQTT-Protokolls.

Jedes Gerät kommuniziert sicher mit dem IoT Hub unter Verwendung von **Shared Access Signatures (SAS-Tokens).** Das SAS-Token ist in den Authentifizierungsheadern des MQTT-Protokolls enthalten. So können nur autorisierte Geräte mit einem gültigen Token eine Verbindung zum IoT Hub herstellen.

Der Azure IoT Hub erzwingt die **TLS**-Verschlüsselung (Transport Layer Security) für alle MQTT-Verbindungen. Zwischen Geräten und der Cloud übertragene Daten sind damit verschlüsselt und vor Abfangen oder Manipulation geschützt. Der TCP-Verkehr verwendet Anschluss 8883 zur Verbindung mit den Servern. DNS: iot-airlinq-airmaster-prod-1.azure-devices.net.

Web-App

Der Zugriff auf die Web-App ist über https://online.airlinq.eu möglich und sie fungiert als Portal, worüber Benutzer auf eine oder mehrere Airmaster-Lüftungsgeräte zugreifen und diese überwachen können. Die Web-App wurde unter Berücksichtigung der

Prinzipien des Responsive Webdesigns entwickelt und ist daher mit nahezu jedem Geräteformfaktor und Betriebssystem kompatibel.

IP-Adresse

Airling L- und P-Steuerbox
Standardmäßig fordert das Lüftungsgerät eine dynamische IP-Adresse von einem DHCP-Server an.
Mit der PC-Software Airlinq Service Tool kann auf jedem Lüftungsgerät eine statische IP-Adresse festgelegt werden.

Airling Aware-Steuerbox (AMX 4)
Standardmäßig fordert das Lüftungsgerät eine dynamische IP-Adresse von einem DHCP-Server an.

Verschlüsselung

Airling L- und P-Steuerbox
Im gesamten System wird verschlüsselt – sowohl zwischen den Lüftungsgeräten und dem Geräte-Gateway als auch zwischen Endbenutzern und der Web-App.
Das Lüftungsgerät kommuniziert mit dem Device Gateway Server über ein unternehmenseigenes Binärprotokoll mit AES128-Verschlüsselung und eindeutigem Schlüssel pro Lüftungsgerät.
Zwischen Endbenutzern und der Web-App (HTTPS) wird eine SSL-Verschlüsselung verwendet.

Airling Aware-Steuerbox (AMX 4)
Der Azure IoT Hub erzwingt die **TLS**-Verschlüsselung (Transport Layer Security) für alle MQTT-Verbindungen. Zwischen Geräten und der Cloud übertragene Daten sind damit verschlüsselt und vor Abfangen oder Manipulation geschützt.

Kommunikation

Airling L- und P-Steuerbox
Das Lüftungsgerät verwendet eine Halbduplex-Kommunikation. Die Schalter der Lüftungsgeräte müssen die Halbduplex-Kommunikation unterstützen.

Das Lüftungsgerät kann nur in einem Netzwerk von 250 Mbit oder darunter kommunizieren. Wird vor Ort eine höhere Geschwindigkeit genutzt, kann ein Schalter mit Halbduplex und Auto-Negotiation eingesetzt werden.

Airling Aware-Steuerbox (AMX 4)
Das Lüftungsgerät verwendet Vollduplex-Kommunikation.