Airlinq® Online : spécifications techniques

Le présent document est destiné aux administrateurs informatiques ou au personnel technique chargés d'établir une connexion entre une ou plusieurs unités de ventilation (ci-après « centrales ») Airmaster et le service en nuage Airlinq® Online.

Aperçu

Airlinq® Online est un service en nuage composé d'un serveur de passerelle et d'une application web.
Le service en nuage est hébergé par Microsoft Azure (Europe de l'Ouest).
Le service en nuage prend en charge toutes les centrales des différents clients et projets. L'accès au service est restreint par une authentification utilisateur.
L'accès et toutes les communications sont chiffrés par défaut (voir la section sur le chiffrement ci-dessous).

Nous conseillons de connecter les centrales à un réseau IoT interne dédié, afin de garantir une séparation avec le réseau utilisé par les PC de bureau et autres appareils. Cette séparation est essentielle pour maintenir l'intégrité et l'efficacité du réseau, et réduire ainsi le risque d'interférences, de vulnérabilités de sécurité et de problèmes de performances entre les centrales et l'équipement de bureau standard.

Serveur de passerelle

Contrôleurs Airling L et P
Le serveur de passerelle gère la communication avec chacune des centrales.
Chaque centrale est préprogrammée pour communiquer avec une certaine adresse de passerelle lorsqu'une connexion Internet est établie via le module Ethernet intégré. La centrale communique ensuite son état à la passerelle en question à intervalles réguliers.

La communication est toujours initiée par les centrales. Il n'est pas nécessaire d'ouvrir un port pour permettre la communication entrante vers les centrales.
La centrale agit comme un client TCP et se connecte aux serveurs de passerelle sur le port 55556. DNS: gateway.airlinq.eu.

En temps normal, une fois la connexion établie, la communication peut circuler librement dans les deux sens jusqu'à la fin de la session et n'est pas limitée par des pare-feu. Certaines organisations appliquent toutefois des politiques de pare-feu fort strictes n'autorisant aucune réponse du serveur de passerelle.
Le client doit alors ajouter une règle ou une exception de pare-feu pour permettre au service Airlinq® Online de fonctionner.

Une communication UDP est utilisée pendant la phase de mise en service pour détecter les centrales sur le réseau interne. Celle-ci ne doit pas nécessairement être prise en charge par le réseau, mais cela facilite le travail des techniciens durant la mise en service.

Contrôleur Airling Aware (AMX 4)
Azure IoT Hub gère la communication avec chacune des centrales.

Azure IoT Hub assure une communication sécurisée entre le centrale et le nuage au moyen de plusieurs mécanismes, notamment en recourant à des jetons d'accès partagés et au protocole MQTT.

Chaque appareil communique avec l'IoT Hub en toute sécurité à l'aide de jetons SAS **(Shared Access Signatures).** Le jeton SAS est inclus dans les en-têtes d'authentification du protocole MQTT. Ainsi, seuls les appareils autorisés disposant d'un jeton valide peuvent établir une connexion à l'IoT Hub.

Azure IoT Hub recourt au chiffrement **TLS (Transport Layer Security)** pour toutes les connexions MQTT. Les données transmises entre les appareils et le nuage sont donc chiffrées et protégées contre toute interception ou altération. Le trafic TCP se connecte aux serveurs sur le port 8883. DNS: iot-airlinq-airmaster-prod-1.azure-devices.net.

Application web

L'application web est accessible sur https://online.airlinq.eu et sert de portail permettant aux utilisateurs d'accéder à une ou plusieurs centrales Airmaster à des fins de surveillance. L'application web est conçue selon les principes du design web réactif, et est donc compatible avec presque tous les appareils et systèmes d'exploitation.

Adresse IP

Contrôleurs Airlinq L et P
Par défaut, la centrale demande une adresse IP dynamique à un serveur DHCP.
Il est possible de définir une adresse IP statique sur chaque centrale à l'aide du logiciel pour PC Airlinq Service Tool.

Contrôleur Airlinq Aware (AMX 4)
Par défaut, la centrale demande une adresse IP dynamique à un serveur DHCP.

Chiffrement

Contrôleurs Airlinq L et P
Le système entier recourt au chiffrement, que ce soit entre les centrales et la passerelle ou entre les utilisateurs finaux et l'application web.
La centrale communique avec le serveur de passerelle à l'aide d'un protocole binaire propriétaire recourant à un chiffrement AES128 avec une clé unique pour chaque centrale.
Le chiffrement SSL est utilisé entre les utilisateurs finaux et l'application web (HTTPS).

Contrôleur Airlinq Aware (AMX 4)
Azure IoT Hub recourt au chiffrement **TLS (Transport Layer Security)** pour toutes les connexions MQTT. Les données transmises entre les appareils et le nuage sont donc chiffrées et protégées contre toute interception ou altération.

Communication

Contrôleurs Airlinq L et P
La centrale utilise une communication en semi-duplex. Les commutateurs des centrales doivent prendre en charge la communication en semi-duplex.

La centrale ne peut communiquer que sur un réseau de 250 Mbit ou moins. Si une vitesse supérieure est utilisée sur le site, il est possible d'utiliser un commutateur avec semi-duplex et négociation automatique.

Contrôleur Airlinq Aware (AMX 4)
La centrale utilise une communication en duplex intégral.