

**Revision: July 2025****Page 1 of 2**

IT Security Documentation

General:

This document contains notes on the Airleader compressor controllers of types 2403, 2404, 3203, 3204, and 0601. It also provides relevant information about the Airleader Online Visualization software.

Data Security:

All data is stored in binary format and can only be read in conjunction with the corresponding software.

Data Exchange:

Data exchange between the controller and the visualization software is carried out via TCP on port 10050. The transmitted data is also transferred in a machine-readable binary format.

Web Interface:

The web interface is accessible via HTTP on port 80 and HTTPS on port 443. HTTP support can be disabled, allowing only SSL access.

A self-signed certificate with RSA 2048 encryption is included. This certificate can be replaced with one certified by your own Certificate Authority (CA).

The GUI is protected by an access code.

Write access is further secured against external access (e.g., man-in-the-middle attacks) by a timestamp/key mechanism.

Open Network Ports:

Inbound:

HTTP:	80
HTTPS:	443
Modbus-TCP:	502 (optional)
OPC-UA:	52530 (optional)

Outbound:

UDP Com Server: 3001 (optional)



Revision: July 2025

Page 2 of 2

IT Security Documentation

OPC UA Security (optional):

The OPC-UA server allows the following access methods:

1. Anonymous: Users are not authenticated
2. Sign: Client is authenticated via certificate
3. Sign & Encrypt: Client is authenticated via certificate, session is encrypted

Airleader Online Visualization:

The Airleader Online Visualization (hereinafter referred to as AOV) is a J2EE application. It is based on an Apache Tomcat server.

The Java Runtime Environment is included in the installation.

Version Information:

Tomcat:	9.0.102
OpenJDK:	1.8.0_352-b08

Additional Components:

Log4J Version:	2.23.1
----------------	--------

Open Network Ports:

HTTP:	8080
HTTPS:	443

AOV also includes a self-signed SSL certificate with RSA 2048 encryption, which can be replaced with a CA-certified certificate.

Both the Tomcat core installation and the Java environment are regularly checked for updates and/or vulnerabilities and updated if necessary. This typically occurs every 6 months or upon discovery of a vulnerability.