TECHNICAL NOTE

LogIQ VDA5050 Analyzer — connecting to the fleet manager

For the administrators of the site

This document describes the connection the analyzer needs, what has to be opened in the firewall for it, and which details we need in order to connect.

Short version: **one outbound MQTT connection to the broker, read-only.** The analyzer behaves like one more MQTT client subscribing to messages — it sends nothing unless proxy mode is deliberately switched on.

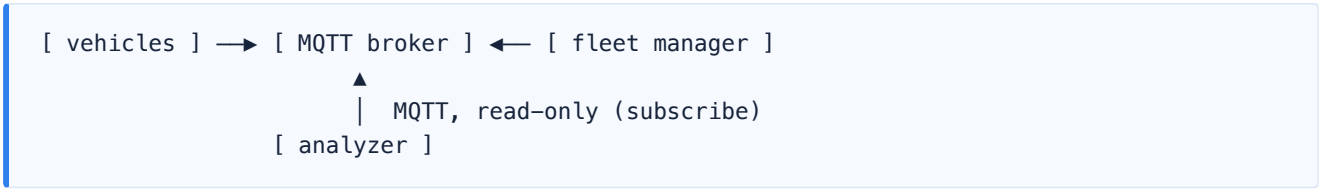
1. How the analyzer is attached

VDA5050 runs over MQTT. Vehicles and fleet manager do not talk to each other directly but through a broker. The analyzer attaches to that broker as an additional client.

Three deployment shapes, which differ in what the firewall has to allow:

A · Analyzer inside your network (on-premise)

The analyzer runs as a Docker container in your network, typically on the same segment as the fleet manager.



Firewall: one internal rule only — from the analyzer host to the broker, TCP 1883, or 8883 if your broker speaks TLS. Nothing needs opening towards the outside. This is the simplest and most frugal variant, and for a site without internet access the only one.

B · Hosted analyzer

The analyzer runs on our side at `vda5050.logistixpert.de`. Your broker then has to be reachable from outside, or a tunnel is laid.

```
[ MQTT broker in your network ] ◀── VPN / SSH tunnel ── [ analyzer, hosted ]
```

Recommended: VPN or SSH tunnel rather than a direct exposure. The analyzer speaks MQTT over TLS (section 4), so the connection itself can be protected — but putting a broker carrying site data on the open internet is a poor idea regardless of this tool, and a tunnel keeps the broker out of everybody's scanner.

If you do want to expose it directly, we will give you the fixed source address to put in your rule on request; it belongs to the hosted analyzer and does not change.

C · Analyzer as a transparent proxy

Optionally the analyzer can sit between vehicles and broker: it accepts the connections and mirrors everything onward to the real broker.

```
[ vehicles ] ──▶ [ analyzer ] ──▶ [ MQTT broker ] ◀── [ fleet manager ]
```

Firewall: additionally inbound to the analyzer host, TCP 1883, from the vehicles. This mode changes the path messages take and is only used by agreement — an analysis does not need it.

---

2. Firewall rules as a table

Shape	Direction	Source	Destination	Port	Protocol
A · on-premise	outbound	analyzer host	MQTT broker	1883 or 8883/TCP	MQTT (TLS)
B · hosted, via VPN	outbound	VPN endpoint	MQTT broker	1883 or 8883/TCP	MQTT (TLS)
B · hosted, direct	inbound	analyzer's fixed address	MQTT broker	8883/TCP	MQTT over TLS
C · proxy (optional)	inbound	vehicles	analyzer host	1883/TCP	MQTT
C · proxy (optional)	outbound	analyzer host	MQTT broker	1883 or 8883/TCP	MQTT (TLS)

Port 8883 is the usual TLS port; the analyzer follows whatever your broker listens on.

Nothing else has to be opened. In particular:

- **No connection to the vehicles.** The analyzer talks to the broker only.
- **No access to the fleet manager**, neither its API nor its database.

- **No outbound internet access** from the site — unless you want the email reports, in which case the analyzer host needs your SMTP server (usually 587/TCP, internal).

Your users reach the analyzer's web interface over HTTPS (443/TCP), or on premise over the port you choose when setting it up (8000/TCP by default).

---

3. What the analyzer does on the broker

So that you can justify a rule, here is exactly what happens on that connection:

- **Connection:** MQTT 3.1.1/5, keepalive 60 seconds. If the connection drops, the client re-establishes it on its own.
- **Subscription:** only the topics entered in the capture profile — usually `uagv/#` or narrower, e.g. `uagv/v2/<manufacturer>/<serial>/#`. QoS 0.
- **Publishing:** none. The analyzer publishes no message to the broker unless proxy mode (shape C) is on. There is no hidden control channel, no instant actions, no orders.
- **Load:** one additional subscriber. On a typical site that is a few hundred kilobit per second, caused by the state messages that flow anyway.
- **Storage:** the recorded messages and the findings go into the analyzer's database. On premise they never leave your network.

A broker account with **read permissions only** is sufficient and is the recommended setup.

---

4. Encryption, and what is not possible today

MQTT over TLS is supported. A capture profile has three settings for it, and they cover what an industrial network actually needs:

- **TLS on or off** — usually port 8883 instead of 1883. The broker's certificate is verified against the system trust store.
- **Your own CA certificate** — the normal case on a site, where the broker's certificate is signed by your own authority and no public root knows about it. Paste the PEM into the profile; it is kept with the profile and used only for that connection.
- **Verification off** — for a self-signed certificate nobody will re-issue for a two-week trial. The traffic stays encrypted; nothing proves who is on the other end, and the profile says so plainly. It is a deliberate choice, never a silent fallback.

The proxy target of a profile (shape C) has the same switch, so a mirrored connection is not quietly weaker than the one it mirrors.

Stated plainly so you do not go looking for it:

- **Client certificates** (mTLS) are not supported yet — the analyzer authenticates with username and password, not with a certificate.
- **Websocket transport** (port 9001 on many brokers) not yet; it has to be the native MQTT port.

Broker credentials are stored encrypted in the analyzer, not in clear text — a capture has to be able to reconnect by itself after a restart.

---

5. What we need from you

These details are enough to set up a connection. The easiest way is to copy the block, fill it in and send it back.

```
Broker
  Host / IP address ......:
  Port ...................:  (1883 plain, 8883 TLS)
  TLS ....................:  no / yes, public CA / yes, own CA
  CA certificate .........:  (PEM, if your own authority signed it)
  Username ...............:  (empty if anonymous is allowed)
  Password ...............:  (please send separately from the rest)
  Read-only account? .....:  yes / no

Topics
  Topics to watch ........:  e.g. uagv/#
  Interface name .........:  e.g. uagv
  Major version in topic .:  e.g. v2

Site
  VDA5050 version ........:  2.1.0 / 3.0
  Number of vehicles .....:
  Manufacturer / serials .:  e.g. Balyo / QA_BALYO_REACHY0001
  Fleet manager ..........:  vendor and version
  M2X peripherals? .......:  yes / no  (load handling, doors, lifts …)

Operation
  Deployment shape .......:  A on-premise / B hosted / C proxy
  For B: route ...........:  VPN / SSH tunnel / direct exposure
  IT contact .............:
```

Useful, but not needed to start:

- The **factsheet** of each vehicle as a JSON file. With it the analyzer checks not only against the standard but against what your vehicle declares it can do. If the vehicles publish their factsheet on the broker, the analyzer picks it up itself.
- The **LIF layout** of the site (VDMA LIF 1.0.0). With it orders are drawn on the real track and checked against the layout.

Please do not send passwords in clear text by email. A second channel is enough: a phone call, Signal, a password link. For a time-boxed trial an account created for the purpose and deleted

afterwards is ideal.

---

6. Testing the path yourself first

Before we connect, you can test the route from the machine the analyzer is to run on. With the Mosquitto tools:

```
mosquitto_sub -h <broker-host> -p 1883 -t 'uagv/#' -v -C 5 -u <user> -P <password>

# with TLS, and your own CA:
mosquitto_sub -h <broker-host> -p 8883 --cafile ca.pem -t 'uagv/#' -v -C 5 -u <user> -P
<password>
```

If five messages arrive, everything the analyzer needs is open. If nothing arrives:

Message	Meaning
`Connection refused`	port closed, or the broker does not listen on that address
Timeout, no message	the firewall is dropping the packets silently
`Connection Refused: not authorised`	the network path is fine, credentials or ACL are not
Connected, no messages	the topic filter does not match, or the account may not read that topic

---

7. Licence, on premises

An installation in your own network carries a signed licence file. It is a small text document: what was bought in readable form, with a signature underneath.

- **No call home.** The licence is checked locally, against a key compiled into the application. A network with no way out is a supported network.
- **Installed in the interface.** Administration → Licence, paste or upload. A file that does not verify is refused before it can replace a working one.
- **Fourteen days of grace** after the end of the term, and after that a read-only installation: everything recorded, every report and every export stays reachable — only new work waits for a current licence.

---

8. Data protection and freedom from interference

- The analyzer reads **machine data** — orders, states, positions, errors. VDA5050 traffic contains no personal data.
- Operation is **free of interference**: a subscriber changes neither the flow of messages nor the behaviour of the vehicles. Only shape C (proxy) sits in the path, and that is agreed explicitly.
- On premise, recordings and reports never leave your network. Hosted, they live on a server in Germany; reports and runs are reachable only through unguessable addresses and after signing in.

Questions about connecting: LogistiXpert · www.logistixpert.de