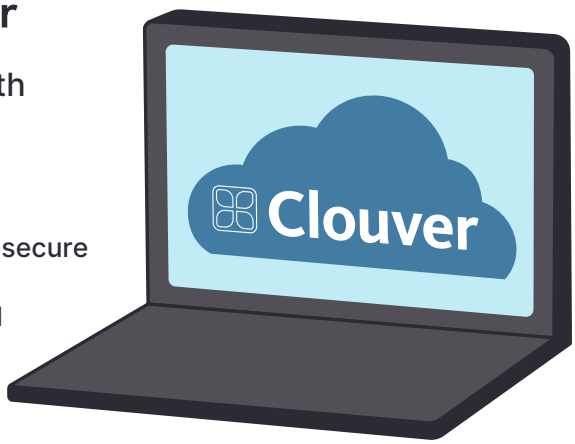
Information on Using the Clouver Cloud

ProCom AUTOMATION

Security Mechanisms in Clouver



There are two secure ways to interact with Clouver:

Browser

Communication via the browser uses HTTPS, the secure variant of HTTP. When connected, messages are transmitted in encrypted form and thus protected from being intercepted by unauthorised parties.

Machines

Machine communication is carried out via the MQTTS protocol, the secure variant of MQTT. During communication, messages are encrypted, which protects them against unauthorised access.

Data Storage and Third-Party Access

- All Clouver data is hosted in certified German data centres.
- The service providers who host Clouver data are only granted authorised access to the customer data in very exceptional cases, strictly for the provision of support services.

Benefits of a Cloud Solution

- With a cloud solution, it is possible to deploy important security updates to all tenants (customer instances) with little effort.
- Should the company's infrastructure be affected by a cyberattack, the cloud solution will remain unaffected.
- A cloud solution allows for easy backups of data in the cloud. This makes the system more resilient in the event of a server hardware failure, as it can simply be switched to a new server.
- A cloud solution is unaffected by any security vulnerabilities that might exist in a company's local network infrastructure.
- Systems in the cloud can be constantly scanned for security flaws, whereas with an edge solution, a security problem can go unnoticed for a long time.