SQL rights required by Unimus

We highly recommend creating a separate SQL user for Unimus for security and access auditing reasons.
After you create your DB (schema) and the user Unimus will use, it will require access to the DB (schema).

Privileges required by the Unimus DB user

On the DB (schema) itself / DDL rights:

- CREATE
- ALTER
- INDEX
- DROP

In each table, for all columns / object rights:

- SELECT
- INSERT
- UPDATE
- EXECUTE
- DELETE

How Unimus stores data in the DB

Any data present in Unimus (including the backups of the devices) are stored in the DB. No data is stored on-disk or anywhere else.
As such, if you want to backup your Unimus data, backing up the DB contents is fully sufficient.

Sensitive data (such as device credentials, API tokens, or any other passwords) are stored encrypted in the DB.
Unimus encrypts data at the application layer using AES-128-CBC using the encryption password setup during the Deployment Wizard.