JUMBO BLOCK INVENTORY

Device and network register for IT and OT



Manual · Version 1.0.0

October 2026

ZANNI GROUP · Andreas Zanni e.K. · Brauhof 12 · 44866 Bochum · jumboblock.org

Contents

1. Overview
2. Basic terms
3. Workflow
4. Creating and opening an inventory
5. Devices
6. Networks and IP plan
7. Sites, contacts and services
8. Certificates
9. Recovery
10. Delivering to the central office
11. Central office: merging units
12. Central specifications
13. File, CSV and verification chain
14. Security and technology
15. Troubleshooting

1. Overview

INVENTORY is the device and network register in the KRITIS area of JUMBO BLOCK. It records sites, networks, devices, contacts, services and certificates – in office IT as well as in the operational technology (OT) of water works, sewage plants, power grids or buildings. The dependencies of devices and services determine the order for recovery after an outage or attack.

In an emergency nobody has to search for the controller's IP address, who is responsible for the firewall, which certificate is expiring or what has to be started up first. The inventory can be printed and works without a network.

Fully offline: INVENTORY runs in the browser, also directly from a USB stick (`file://`). There is no server connection, no account and no cloud. The inventory file is encrypted with your password.

For municipalities and companies with several units: every unit – a department, a plant, an operating division – keeps its own inventory and delivers it encrypted and signed to a central office. The central office merges the partial inventories and can in turn deliver to a higher level.

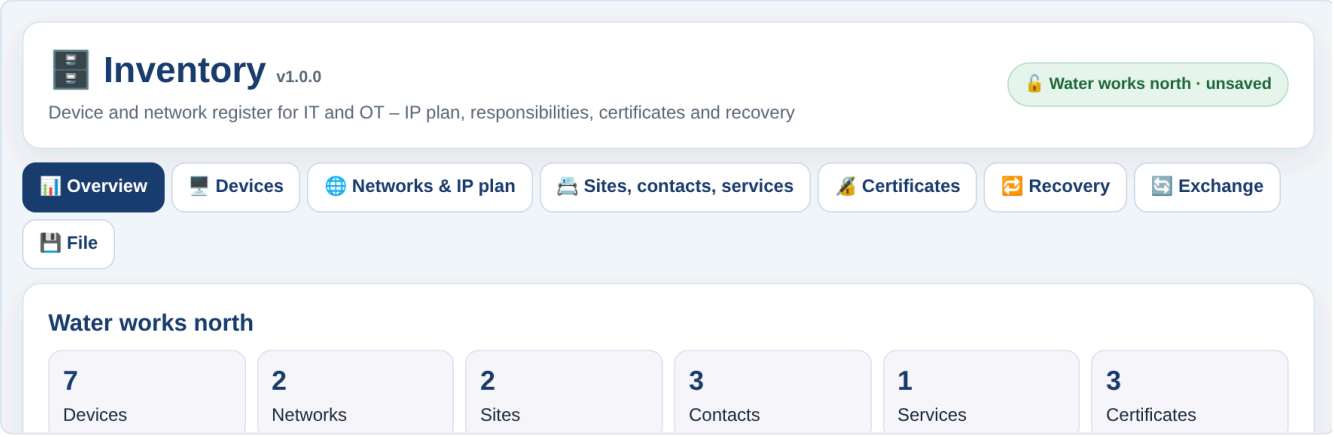


Fig. 1: INVENTORY work area with overview

Area	Purpose
Overview	Number of objects, notes and warnings, subordinate units
Devices	Servers, workstations, network equipment, PLCs, control systems, field devices, UPS and more
Networks & IP plan	Networks with zone, VLAN, gateway, DNS and DHCP; IP plan with usage and free ranges
Sites, contacts, services	Buildings, rooms and cabinets; people, service providers and authorities; critical services and business processes
Certificates	Certificates from your own CA (JUMBO BLOCK CERT) or from files, with expiry warning
Recovery	Order from the dependencies; tick off recovery step by step in an emergency
Exchange	Deliveries to the central office, receiving, return deliveries and specification packages
File	Save, lock, CSV import and export, verification chain

2. Basic terms

Term	Meaning
Inventory	Encrypted file (.dbm) of a unit with all objects, delivery states and the verification chain
Unit	Organisational unit that keeps its own inventory, e.g. “Water works north” or “Public order office”
Object	An entry of the types site, network, device, contact, service or certificate. Objects refer to each other, e.g. device → site, responsible person, services.
Dependency (“needs …”)	A device or service can only run once the specified devices or services are running. This results in the recovery stages.
Central office	Unit that merges the partial inventories of subordinate units
Delivery	Encrypted and signed package (.jbc) with a unit's partial inventory to the central office
Return delivery	Package from the central office to a unit with the partial inventory edited by the central office. It completely replaces the unit's partial inventory.
Specification package	Package from the central office to all units with shared master data, assigned IP ranges and delivery interval
Verification chain	Hash chain of all changes and exchange operations in the inventory

3. Workflow

Single unit

1. Create the inventory (chapter 4).
2. Record master data: sites, contacts, services (chapter 7) – or take over existing lists via CSV (chapter 12).
3. Record networks and devices, with IP addresses, responsible persons and dependencies (chapters 5 and 6).
4. Import certificates from the CERT CA file (chapter 8).
5. Work through notes and warnings in the overview, check and print the recovery order (chapter 9).
6. Save and put a copy together with printouts in the emergency folder.

Several units with a central office

1. Every unit and the central office have an identity in the JUMBO BLOCK CRYPT keyring and exchange their public keys (.jbid).
2. The central office registers the units, the units set the central office – each with fingerprint comparison.
3. The units deliver their partial inventory at the agreed interval; the central office verifies and takes it over (chapter 10).
4. The central office distributes specifications and sends changes back as a return delivery (chapter 11).

4. Creating and opening an inventory

1. Under *New inventory* enter the name of the unit, a short code and the organisation.
2. Enter a password of at least 12 characters twice.
3. Click *Create inventory* and save afterwards.

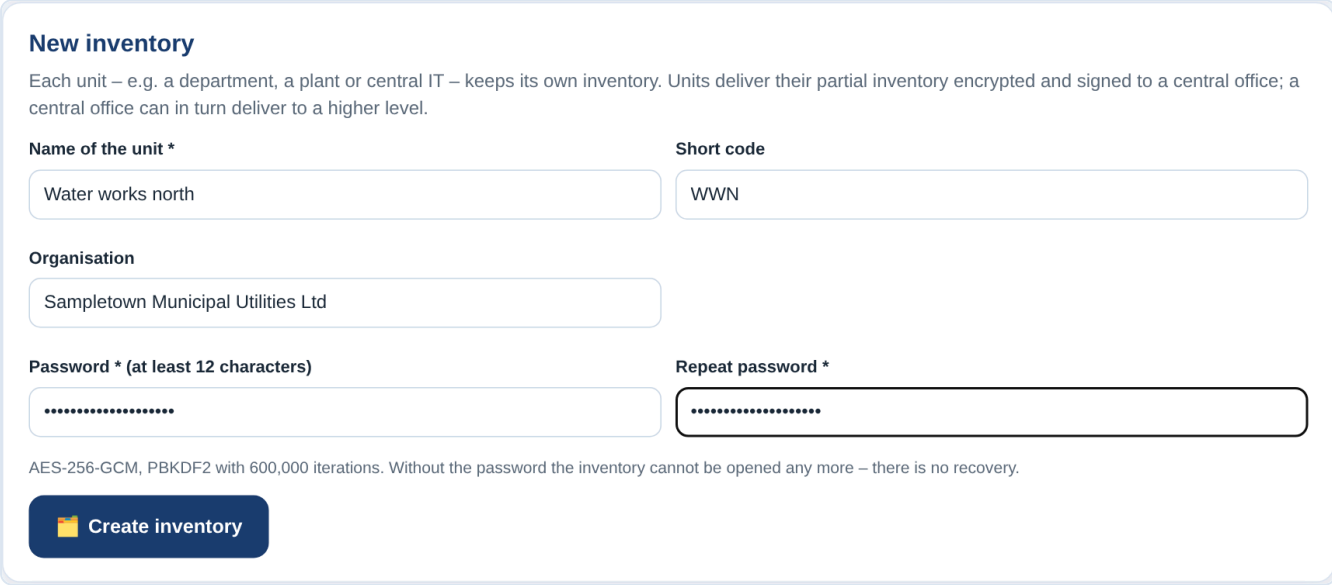


Fig. 2: Creating a new inventory

> Without the password the inventory cannot be opened any more – there is no recovery.

- *Open inventory* reads an existing file; the password is requested afterwards.
- The inventory locks after 15 minutes without input; the password is enough to continue.
- Until saved, it is additionally cached encrypted in the browser and offered for restoration on the start page after a crash.

Overview

After opening, the overview shows the number of objects, unit, role and integrity value as well as all notes and warnings.



Fig. 3: Overview with number of objects and integrity value



Fig. 4: Notes and warnings

Check	Example
IP addresses	assigned twice, outside all recorded networks, outside the ranges assigned by the central office; overlapping networks
Devices	end of support passed, serial number recorded several times, no responsible person, critical device without recovery check
Certificates	expired, revoked or expiring within 30 days
Dependencies	reference to a non-existent object, circular dependency
Exchange	delivery to the central office due, delivery from a unit overdue, return delivery pending

5. Devices

The *Devices* tab lists all devices and systems with type, IP addresses, site, firmware and responsible person. Search finds name, IP address, vendor and serial number; the type filter narrows the list. A passed end of support is marked with *EOL*.

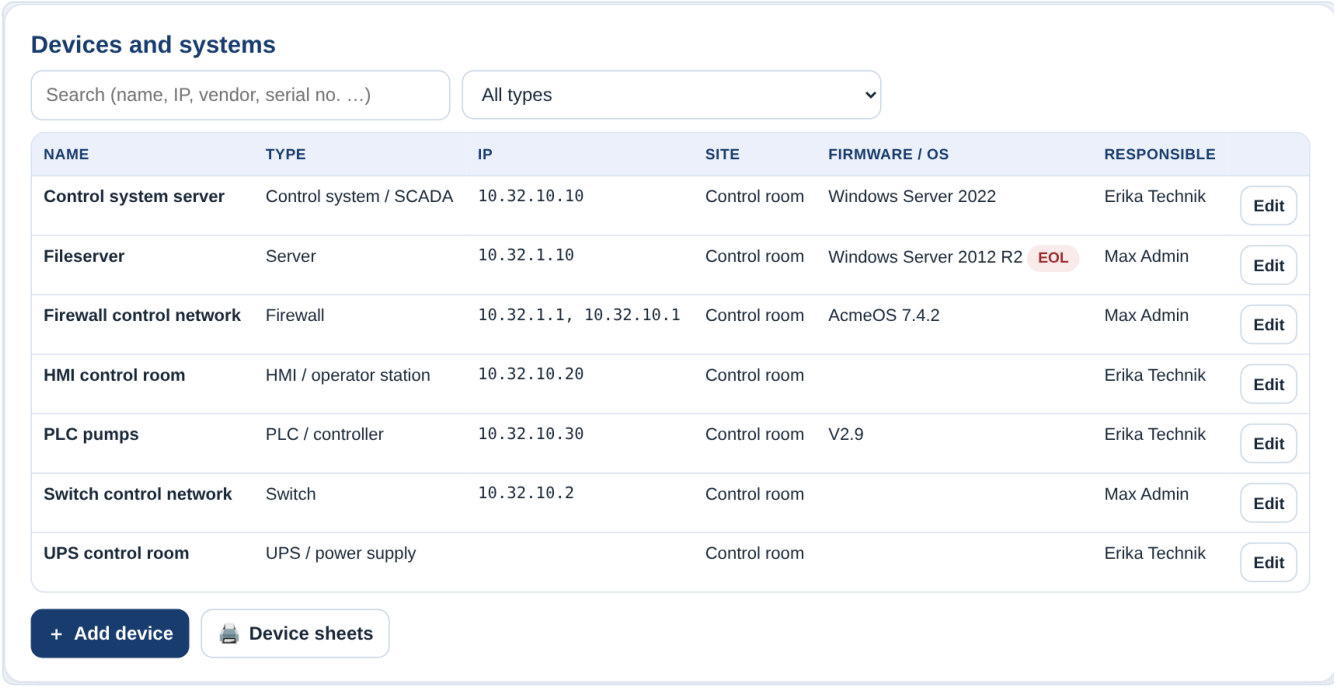


Fig. 5: Devices of a water works

Add device or *Edit* opens the form.

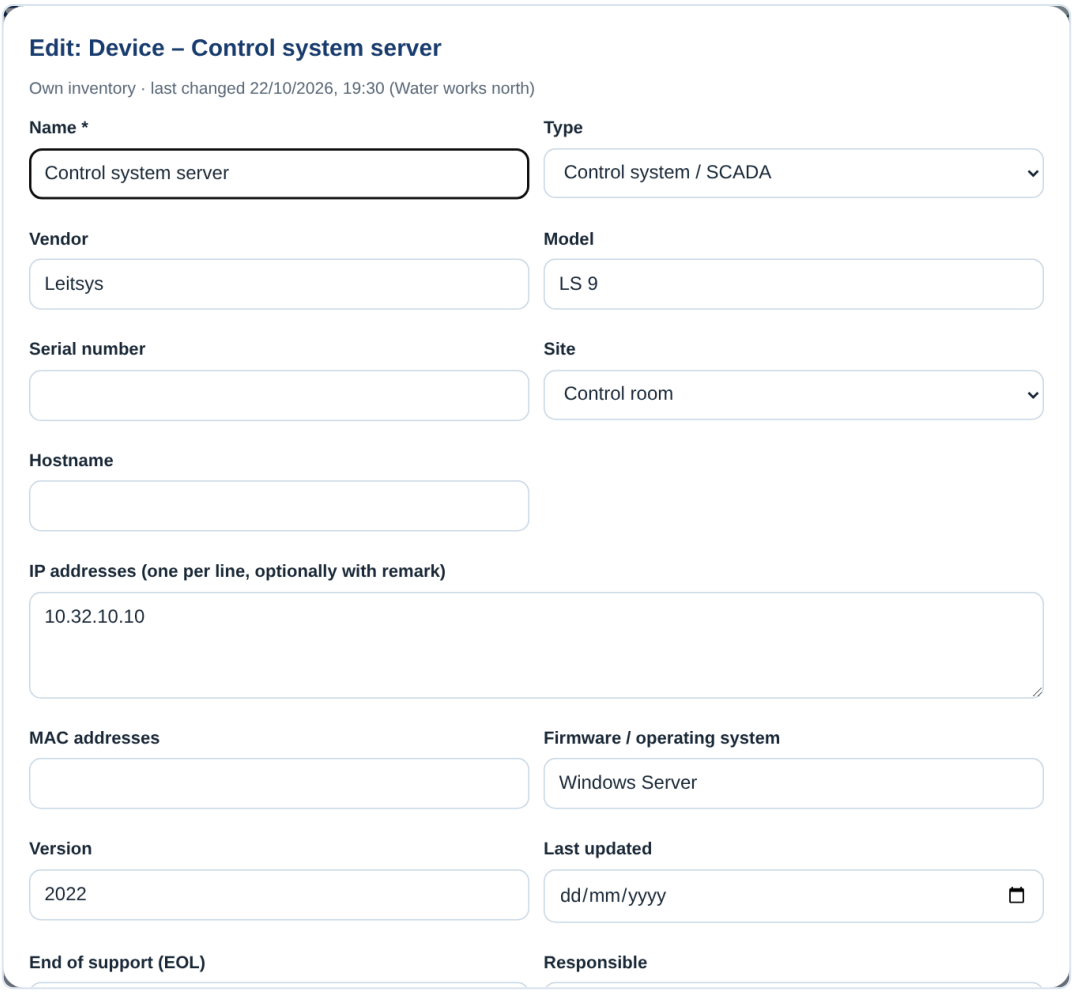


Fig. 6: Device form (excerpt)

Field group	Fields
Identification	Name, type (18 types from server via PLC, HMI and control system to field device and UPS), vendor, model, serial number, site
Network	Hostname, IP addresses (one per line, optionally with remark), MAC addresses
Software	Firmware or operating system, version, last updated, end of support (EOL)
Responsibility	Responsible, deputy, supplier / maintenance, maintenance contract
Importance	Criticality, supports services, needs (dependencies)
Access	Only a reference, e.g. to an entry in JUMBO BLOCK VAULT – no passwords
Recovery	Priority within the stage, target time, check criterion “running when …”, steps or manual

References to sites, contacts, devices and services are chosen from selection lists; for *needs* and *services* multiple selection with `Ctrl` or ⌘ is possible. An object that is still referenced cannot be deleted.

Device sheets prints one sheet with all details per device – for the emergency folder or for attaching to the control cabinet.

Never enter passwords in the *Access* field. Access data belongs in a password vault such as JUMBO BLOCK VAULT.

6. Networks and IP plan

Networks are recorded with name, zone (IT / office, OT / production / control, DMZ, management, guest, other), network in CIDR notation (e.g. `10.32.10.0/24`), VLAN, gateway, DNS servers, DHCP range, site and responsible person. An address such as `10.32.1.17/24` is corrected to the network address `10.32.1.0/24`.

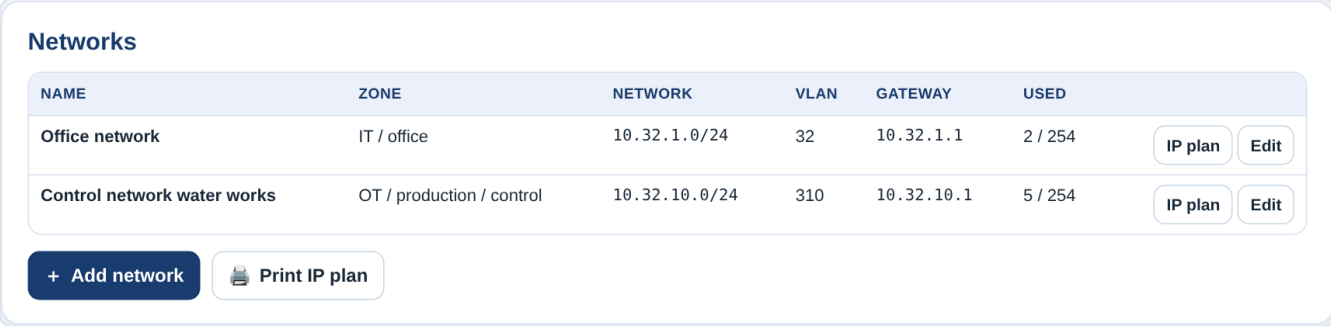


Fig. 7: Networks with zone, VLAN, gateway and usage

IP plan shows all used addresses of a network with device, the number of used and free addresses and the free ranges. *Print IP plan* creates the plan of all networks for printing.

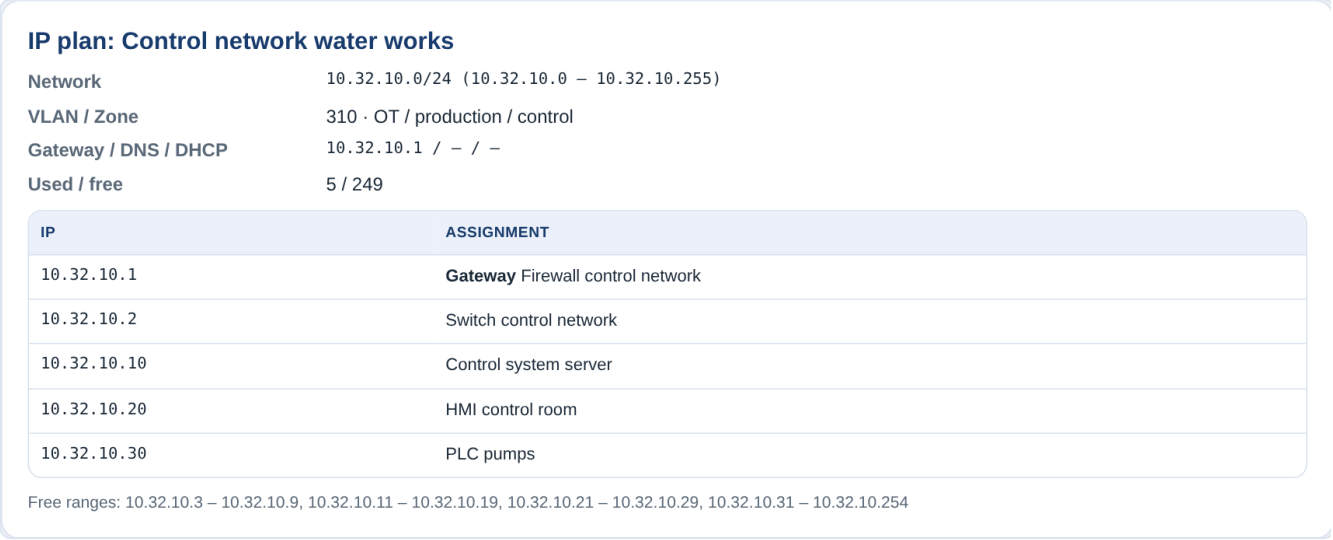


Fig. 8: IP plan of the control network with usage and free ranges

> Addresses assigned twice and addresses outside the recorded networks appear as warnings in the overview.

7. Sites, contacts and services

The *Sites, contacts, services* tab combines the master data; the switch selects the type.

Type	Fields
Sites	Name, type (building, room, cabinet / rack, data centre, outdoor facility), address, located in (parent site), access (keys, entry), note
Contacts	Name, type (person, service provider / supplier, authority), function, telephone, mobile, e-mail, availability / on-call, contract or customer number
Services	Critical service or business process with description, criticality, responsible person, “needs …” and recovery details, e.g. “available when network pressure > 4 bar”

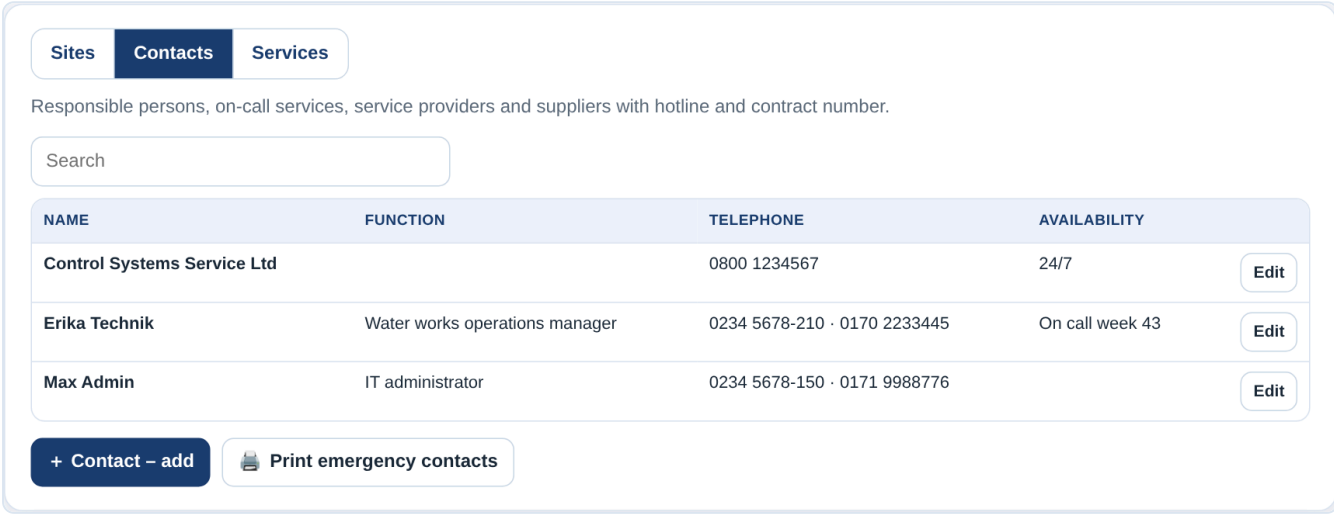


Fig. 9: Contacts with availability

Print emergency contacts creates a list of all contacts with telephone, mobile, availability and the devices, networks and services they are responsible for.

8. Certificates

In an emergency, expired certificates paralyse operator interfaces, remote maintenance and interfaces. INVENTORY therefore keeps all certificates with expiry date and assignment to a device.

- *Import register from CA file (Cert)* reads the JUMBO BLOCK CERT CA file. Only the register is read – no password is needed; the CA's private key stays encrypted. When read in again, existing entries are updated, e.g. revoked certificates.
- *Load certificate file (.crt, .pem)* imports individual certificates, also from other issuers.
- *Add manually* for certificates whose file is not available.

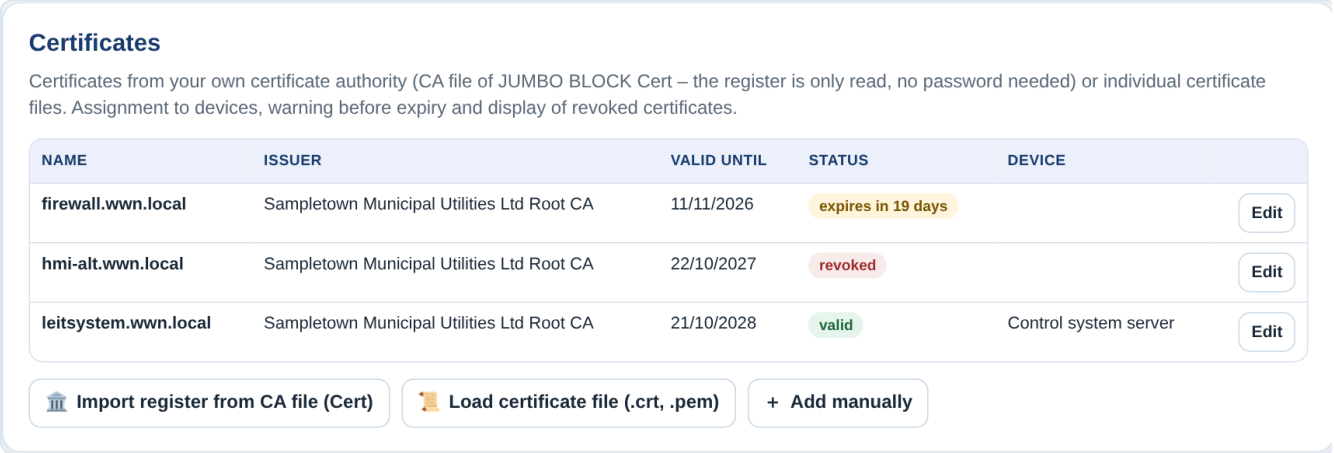


Fig. 10: Certificates with status and assigned device

The *Status* column shows valid, expires in … days (from 30 days before expiry), expired or revoked. *Edit* assigns the certificate to a device.

9. Recovery

From the “needs …” details of all devices and services, INVENTORY calculates the recovery order in stages: stage 1 contains everything that needs nothing else, stage 2 everything that only needs stage 1, and so on. Within a stage the priority decides.

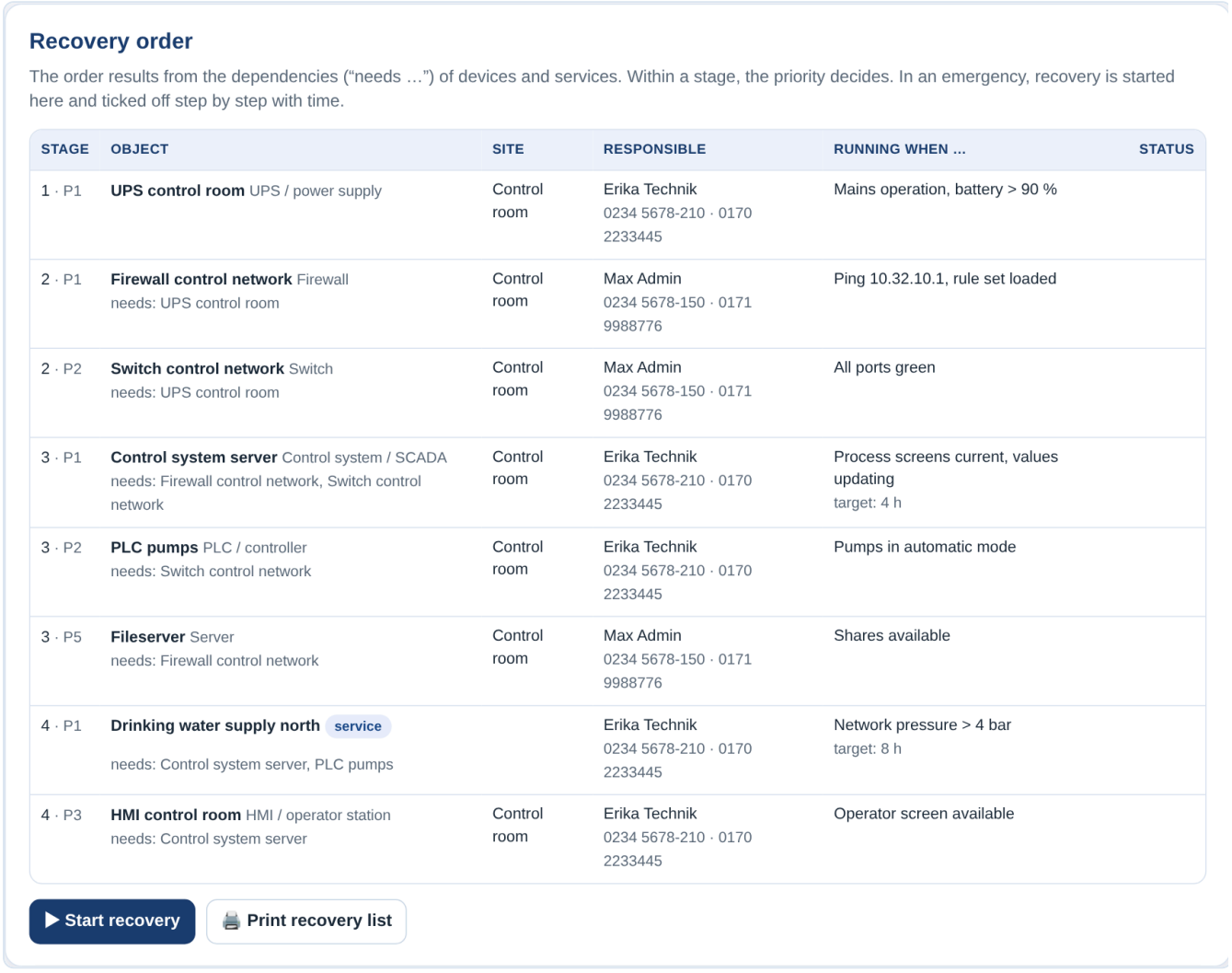


Fig. 11: Recovery order with stages, responsible persons and check criteria

For each object the list shows site, responsible persons with telephone and the check criterion “running when …” with target time. A circular dependency is reported because no order can be determined then. *Print recovery list* creates a list for ticking off with a column for time and initials.

In an emergency

1. *Start recovery* – state occasion and lead.
2. Set the status for each object: ▶️ starting up, ✅ running, ⚠️ problem (with note). The time is recorded. Objects whose prerequisites are not yet running show “waiting for …”.
3. With *Report status to the situation log* send the current status as an encrypted message to JUMBO BLOCK LOGBOOK – load the log's message key (.jbk) once for this.
4. When finished, *End recovery*.

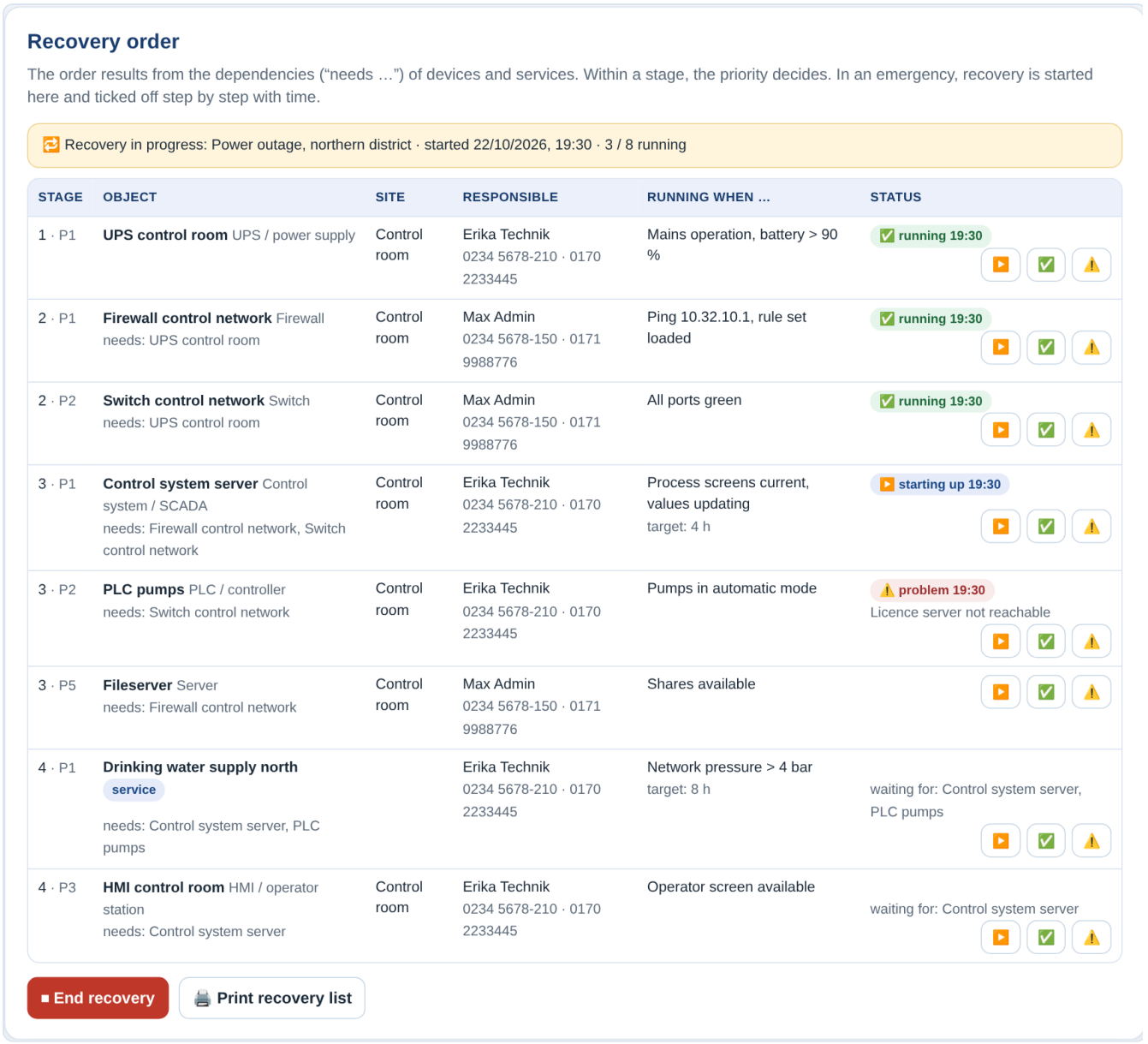


Fig. 12: Recovery in progress with status per object

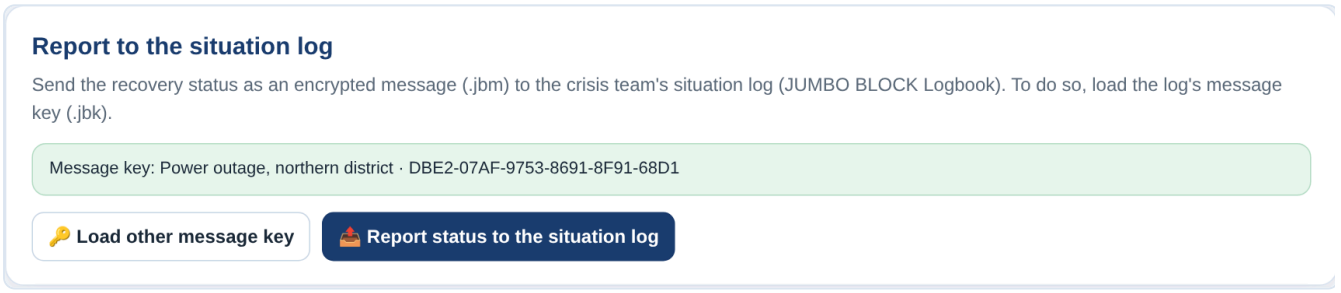


Fig. 13: Message to the situation log

Start, every status change, messages to the situation log and the end are recorded in the verification chain.

10. Delivering to the central office

Deliveries are encrypted and signed with an identity from the JUMBO BLOCK CRYPT keyring. The keyring is loaded in the *Exchange* tab with *Open keyring …*; it only stays open until locking and is not changed.

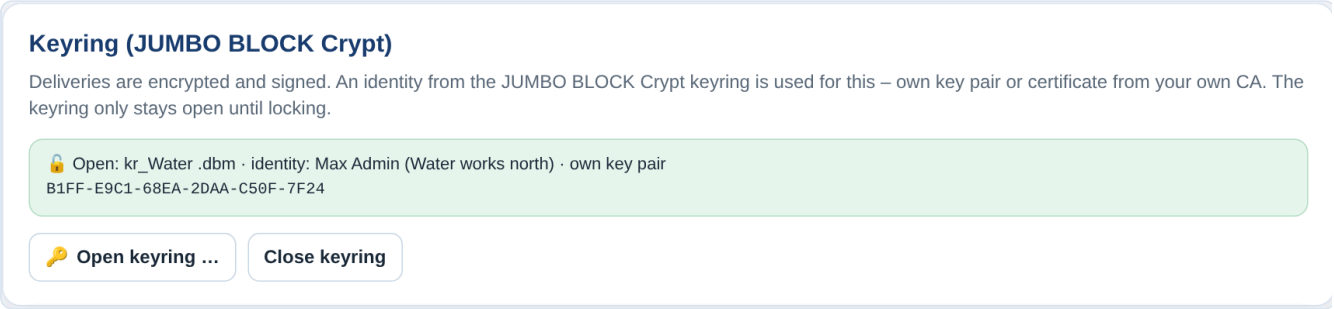


Fig. 14: Open keyring with selected identity

Setting the central office

Set central office (.jbid) … loads the central office's public key. Compare the fingerprint with the central office – by phone or in person. Afterwards, only packages with exactly this key are accepted as return delivery or specifications.

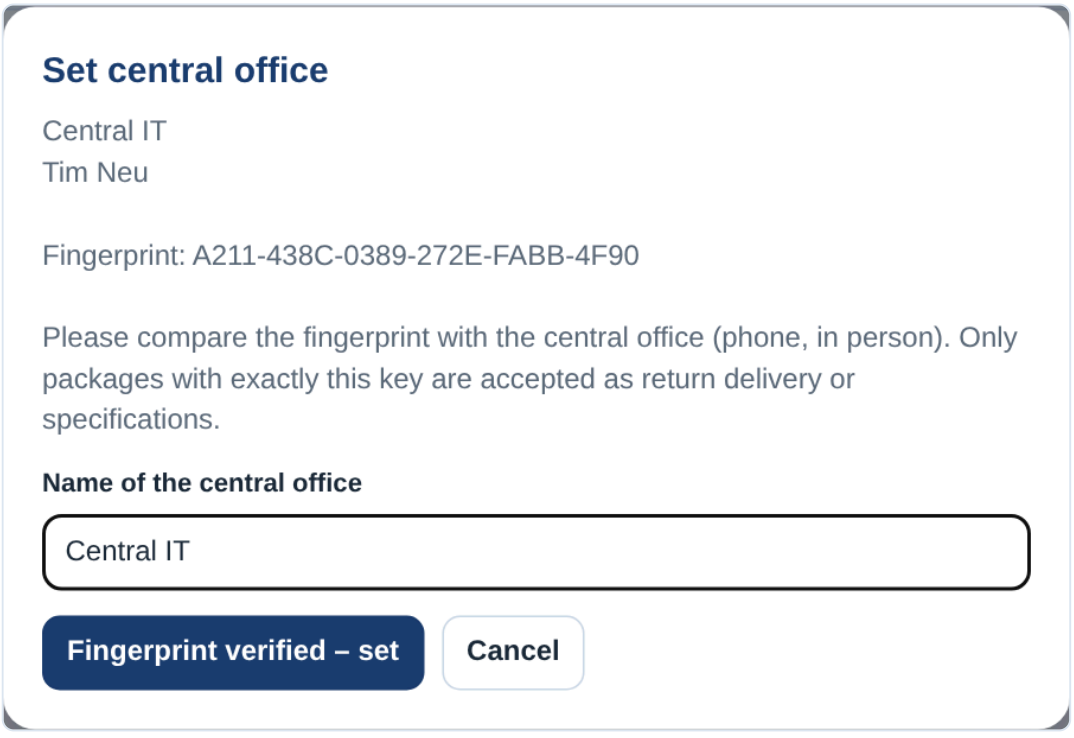


Fig. 15: Setting the central office with fingerprint comparison

Creating a delivery

The *Deliver to the central office* area shows the central office, the last delivery state and the number of changes since the last delivery. *Create delivery* produces the package (.jbc), which you hand to the central office. *Own public key (.jbid)* saves the key the central office needs to register the unit.

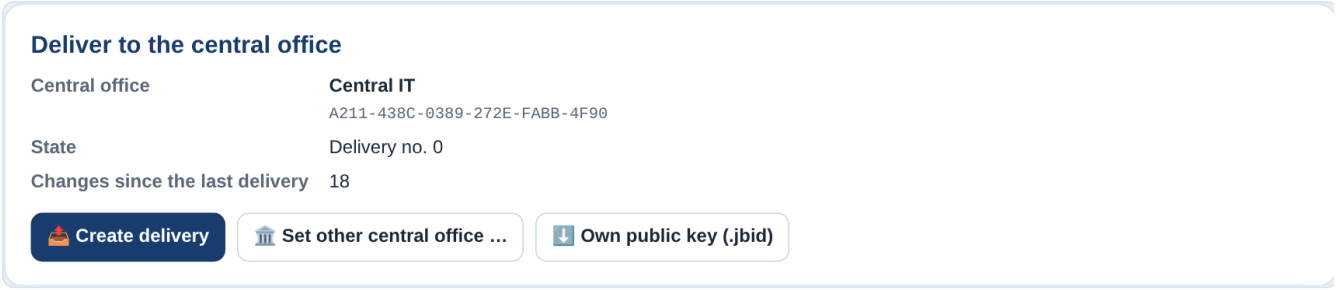


Fig. 16: Delivering to the central office

If the central office specifies a delivery interval, the overview points out a due delivery.

11. Central office: merging units

Registering units

- *Add unit (.jbid)* loads a unit's public key. After comparing the fingerprint, it is registered with a name. Only deliveries with exactly this key are assigned to it.
- *Unit without Inventory (CSV)* takes over the list of a unit that does not use INVENTORY itself.

Receiving deliveries

Read package (.jbc) detects the package type, verifies encryption, signature, sender and continuity with the last state and shows all changes compared to the previous state.

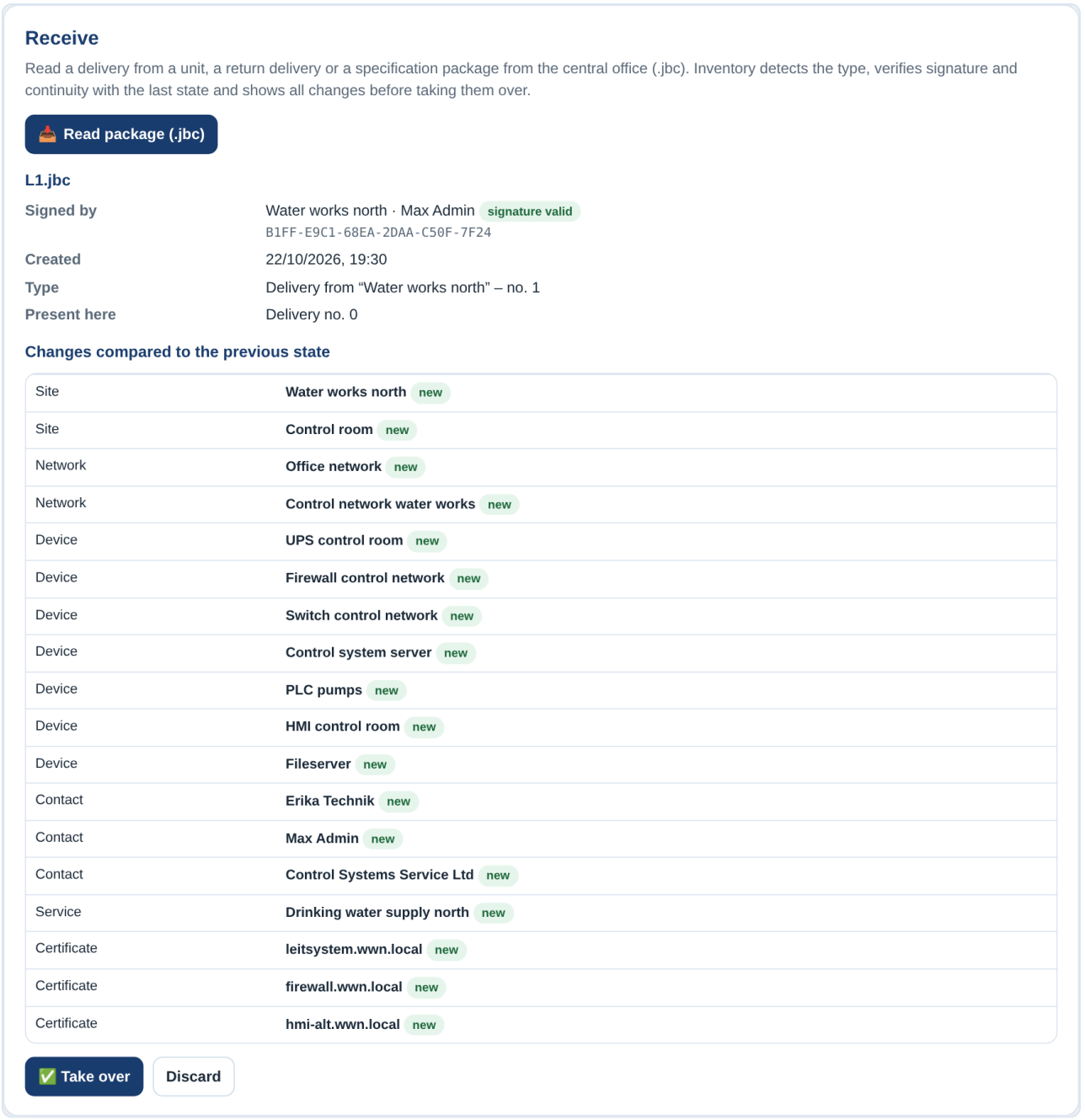


Fig. 17: Delivery from a unit with changes

Take over merges the partial inventory into the overall inventory; *Discard* rejects the delivery. Both are logged. Deliveries from unknown senders, altered or unsigned packages and older states are rejected.

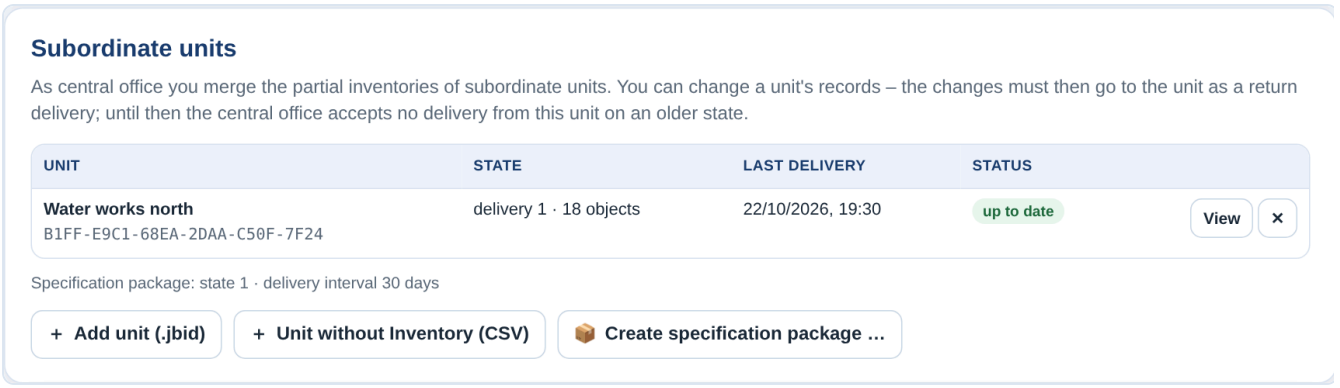


Fig. 18: Subordinate units with delivery state

Choosing the view

Via *View* the central office switches between its own inventory, the read-only *Overall view (all units)* and the partial inventory of a single unit. In the overall view every object carries the name of its unit.

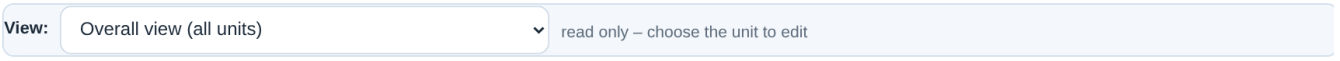


Fig. 19: Selecting the view

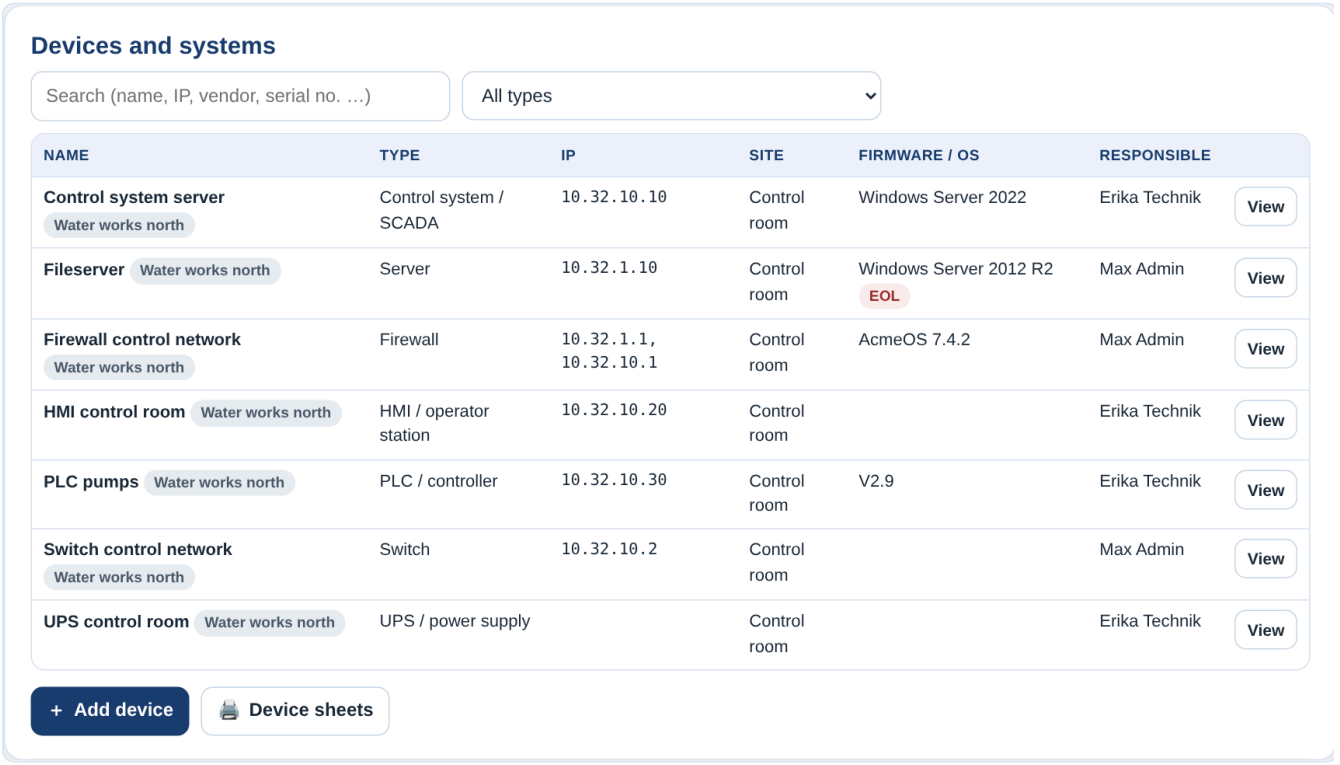


Fig. 20: Overall view of the devices of all units

Changing a unit's data and return delivery

The central office may change a unit's records. These changes must go to the unit as a **return delivery**: until the unit has imported it, the central office accepts no delivery from this unit on an older state. At the unit, the return delivery completely replaces the previous partial inventory. INVENTORY then offers the

unit's own changes made since its last delivery individually for re-application – preselected if there is no conflict; in case of conflict the unit decides deliberately.

12. Central specifications

Create specification package … produces a package for all registered units. It contains the central office's sites, networks, devices, contacts and services (without certificates), the IP ranges assigned to each unit and the delivery interval in days.

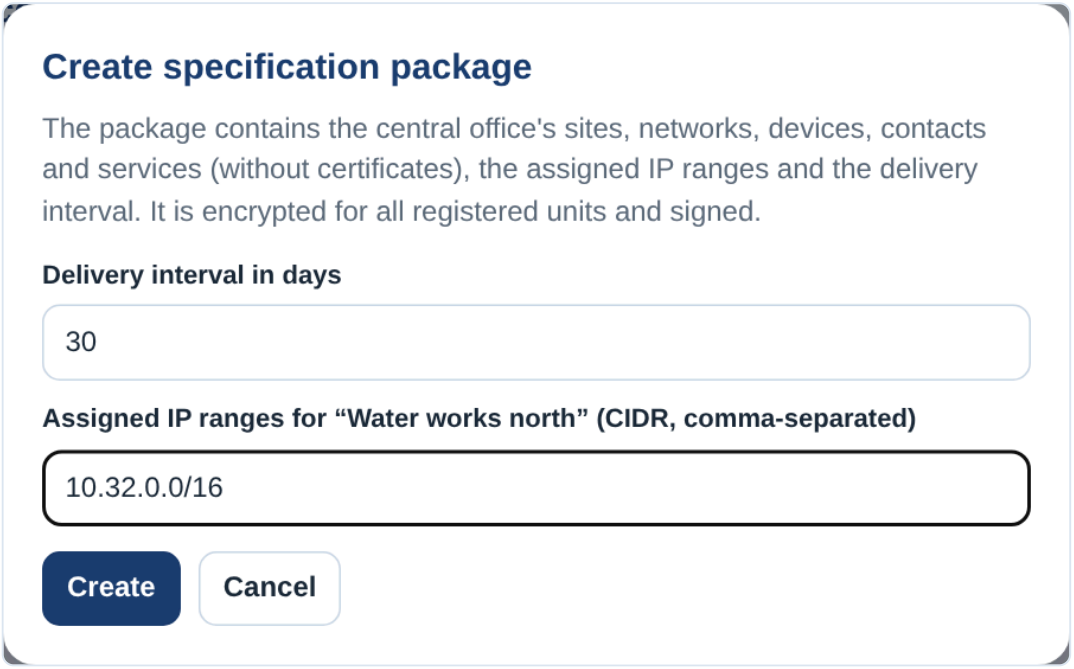


Fig. 21: Specification package with delivery interval and assigned IP ranges

At the unit the package is imported via *Read package*. The specifications appear grey and read-only, e.g. central DNS servers or contacts of central IT. Own objects can refer to them. IP addresses outside the assigned ranges are shown as warnings.

A specification package is only accepted if it is signed by the configured central office and carries a newer state. If no central office is set yet, importing sets the sender as central office – compare the fingerprint beforehand.



Fig. 22: Overall view of the central office

13. File, CSV and verification chain

Inventory file

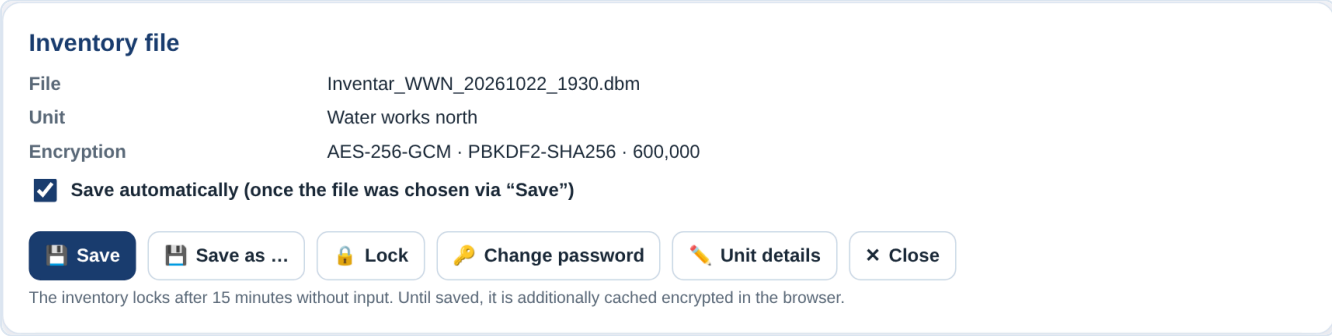


Fig. 23: Inventory file

Button	Effect
Save / Save as …	Saves encrypted; in Chrome and Edge with *Save automatically* after every change
Lock · Change password · Close	As in the other programs of the suite
Unit details	Change name, short code and organisation of the unit

CSV import and export

Existing lists, e.g. from Excel, can be taken over. Choose the type; *Export CSV* provides a template with the column names. For import, the first line must contain column names as in the export file; separator semicolon or comma. References to sites and contacts are matched by name, and missing ones are created automatically. Unmatched columns are reported.

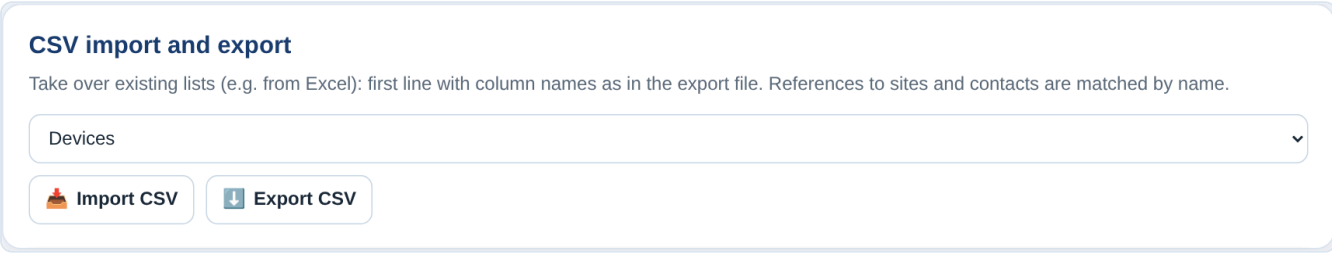


Fig. 24: CSV import and export

Verification chain

Every change to objects, every exchange and every recovery is recorded with time and SHA-256 hash. The verification chain additionally secures the data state of every view. When opening, INVENTORY checks whether chain and data match.

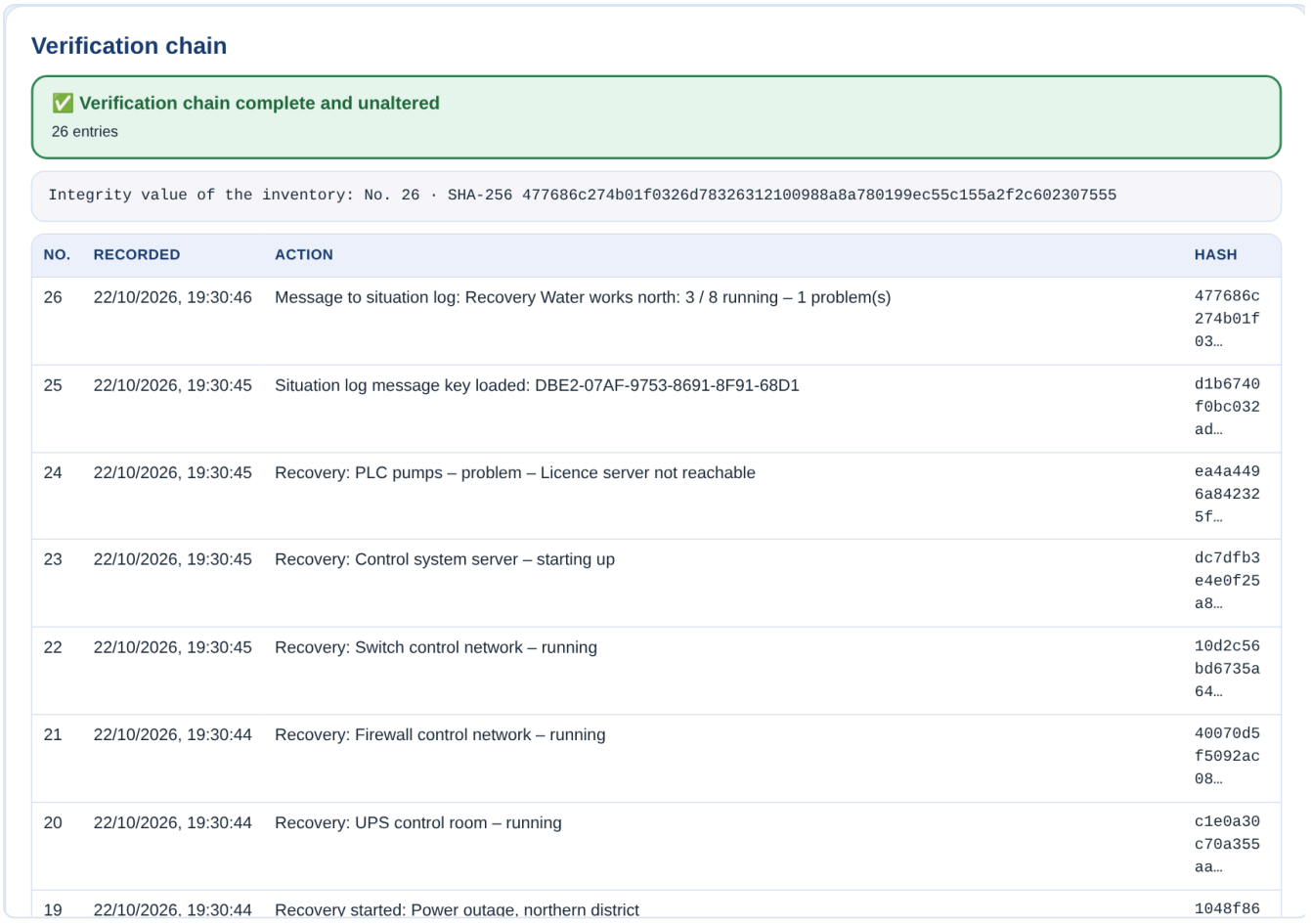


Fig. 25: Verification chain

14. Security and technology

Area	Implementation
Inventory file	AES-256-GCM, PBKDF2-SHA-256 with 600,000 iterations; additional SHA-256 checksum of the file
Packages	JUMBO BLOCK CRYPT file format (.jbc): ECDH P-256, HKDF-SHA-256 and AES-256-GCM for the recipients, sender's signature with ECDSA or RSA
Assignment	Units and central office are recognised by their key fingerprint; delivery states by sequence numbers and checksums
Verification chain	SHA-256 per entry with predecessor hash, starting with “GENESIS”, including the hash of the data state
Messages	Recovery messages in the JUMBO BLOCK LOGBOOK format, encrypted with the log's message key
Privacy	No network connection, no telemetry; no passwords in the inventory

Limits

- INVENTORY does not search the network for devices itself. The data is only as good as its maintenance – check and deliver regularly.
- The inventory is a sensitive file: it describes networks, addresses and responsibilities. Treat printouts like access data.
- Several people working in the same file at the same time is not intended; units and deliveries exist for this.

15. Troubleshooting

Problem	Cause and solution
“Please enter the network in CIDR notation”	Enter the network as an address with prefix, e.g. `10.20.1.0/24`.
“Still referenced by …” when deleting	First remove the references in the objects named.
“Circular dependency in recovery”	Two objects need each other. Remove one of the dependencies.
“The package is not encrypted for an identity of this keyring”	Wrong keyring opened or package for another unit. Open the correct keyring.
“The sender is not registered as a subordinate unit”	First register the unit with its public key (.jbid).
Delivery rejected because of unsent central changes	First create the return delivery or discard the changes; the unit then delivers on the new state.
“This specification package has already been imported or is outdated”	A newer specification package has already been imported. No action required.
CSV import: “No column Name found”	The first line must contain the column names; create a template with *Export CSV*.
“Verification chain broken”	The file was changed outside INVENTORY. Compare with a backup.