JUMBO BLOCK INVENTORY

Geräte- und Netzregister für IT und OT



Handbuch · Version 1.0.0

Oktober 2026

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

Inhalt

1. Überblick
2. Grundbegriffe
3. Arbeitsablauf
4. Inventar anlegen und öffnen
5. Geräte
6. Netze und IP-Plan
7. Standorte, Kontakte und Dienste
8. Zertifikate
9. Wiederanlauf
10. Lieferung an die Zentrale
11. Zentrale: Stellen zusammenführen
12. Vorgaben der Zentrale
13. Datei, CSV und Prüfkette
14. Sicherheit und Technik
15. Fehlerbehebung

1. Überblick

INVENTORY ist das Geräte- und Netzregister im KRITIS-Bereich von JUMBO BLOCK. Es erfasst Standorte, Netze, Geräte, Kontakte, Dienste und Zertifikate – in der Büro-IT ebenso wie in der Betriebstechnik (OT) von Wasserwerken, Kläranlagen, Stromnetzen oder Gebäuden. Aus den Abhängigkeiten der Geräte und Dienste ergibt sich die Reihenfolge für den Wiederanlauf nach einem Ausfall oder Angriff.

Im Ernstfall muss niemand mehr suchen, welche IP-Adresse die Steuerung hat, wer für die Firewall zuständig ist, welches Zertifikat abläuft oder was zuerst wieder hochgefahren werden muss. Das Inventar ist ausdruckbar und funktioniert ohne Netz.

Vollständig offline: INVENTORY läuft im Browser, auch direkt vom USB-Stick (`file://`). Es gibt keine Server-Verbindung, kein Konto und keine Cloud. Die Inventardatei ist mit Ihrem Passwort verschlüsselt.

Für Kommunen und Unternehmen mit mehreren Stellen: Jede Stelle – ein Amt, ein Werk, ein Betriebsteil – führt ihr eigenes Inventar und liefert es verschlüsselt und signiert an eine Zentrale. Die Zentrale führt die Teil-Inventare zusammen und kann selbst wieder an eine höhere Ebene liefern.

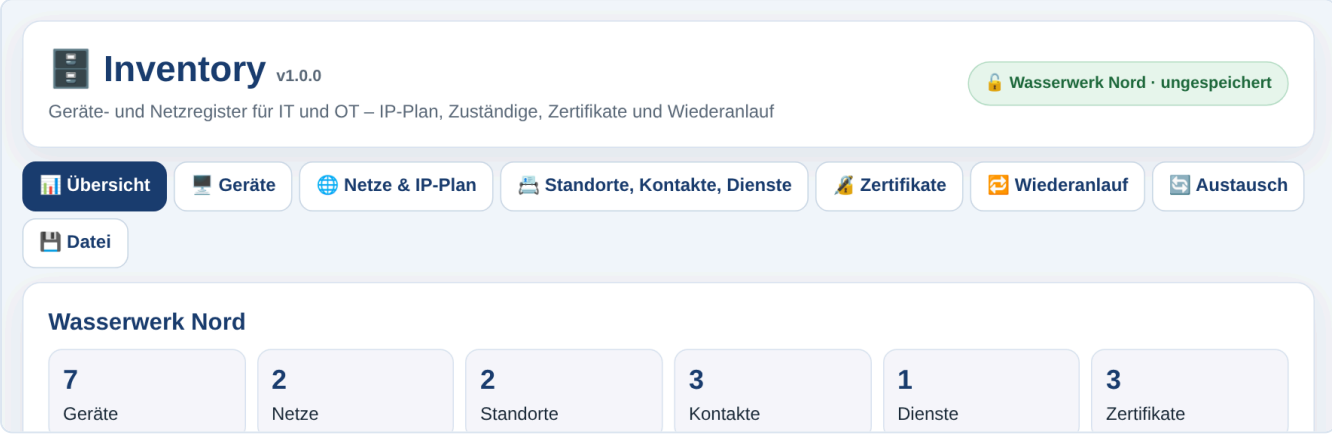


Abb. 1: Arbeitsbereich von INVENTORY mit Übersicht

Bereich	Aufgabe
Übersicht	Anzahl der Objekte, Hinweise und Warnungen, untergeordnete Stellen
Geräte	Server, Arbeitsplätze, Netzwerktechnik, Steuerungen, Leitsysteme, Feldgeräte, USV und mehr
Netze & IP-Plan	Netze mit Zone, VLAN, Gateway, DNS und DHCP; IP-Plan mit Belegung und freien Bereichen
Standorte, Kontakte, Dienste	Gebäude, Räume und Schränke; Personen, Dienstleister und Behörden; kritische Dienstleistungen und Geschäftsprozesse
Zertifikate	Zertifikate aus der eigenen CA (JUMBO BLOCK CERT) oder aus Dateien, mit Ablaufwarnung
Wiederanlauf	Reihenfolge aus den Abhängigkeiten; Wiederanlauf im Ernstfall Schritt für Schritt abhaken
Austausch	Lieferungen an die Zentrale, Empfang, Rücklieferungen und Vorgabepakete
Datei	Speichern, Sperren, CSV-Import und -Export, Prüfkette

2. Grundbegriffe

Begriff	Bedeutung
Inventar	Verschlüsselte Datei (.dbm) einer Stelle mit allen Objekten, Lieferständen und der Prüfkette
Stelle	Organisationseinheit, die ihr eigenes Inventar führt, z. B. „Wasserwerk Nord“ oder „Ordnungsamt“
Objekt	Ein Eintrag der Arten Standort, Netz, Gerät, Kontakt, Dienst oder Zertifikat. Objekte verweisen aufeinander, z. B. Gerät → Standort, Verantwortlich, Dienste.
Abhängigkeit („braucht …“)	Ein Gerät oder Dienst kann erst laufen, wenn die angegebenen Geräte oder Dienste laufen. Daraus entstehen die Stufen des Wiederanlaufs.
Zentrale	Stelle, die Teil-Inventare untergeordneter Stellen zusammenführt
Lieferung	Verschlüsseltes und signiertes Paket (.jbc) mit dem Teil-Inventar einer Stelle an die Zentrale
Rücklieferung	Paket der Zentrale an eine Stelle mit dem von der Zentrale bearbeiteten Teil-Inventar. Es ersetzt das Teil-Inventar der Stelle vollständig.
Vorgabepaket	Paket der Zentrale an alle Stellen mit gemeinsamen Stammdaten, zugewiesenen IP-Bereichen und Lieferturnus
Prüfkette	Hash-Kette aller Änderungen und Austauschvorgänge im Inventar

3. Arbeitsablauf

Einzelne Stelle

1. Inventar anlegen (Kapitel 4).
2. Stammdaten erfassen: Standorte, Kontakte, Dienste (Kapitel 7) – oder vorhandene Listen per CSV übernehmen (Kapitel 12).
3. Netze und Geräte erfassen, mit IP-Adressen, Verantwortlichen und Abhängigkeiten (Kapitel 5 und 6).
4. Zertifikate aus der CA-Datei von CERT übernehmen (Kapitel 8).
5. Hinweise und Warnungen in der Übersicht abarbeiten, Wiederanlaufreihenfolge prüfen und ausdrucken (Kapitel 9).
6. Speichern und eine Kopie samt Ausdrucken in den Notfallordner legen.

Mehrere Stellen mit Zentrale

1. Jede Stelle und die Zentrale haben eine Identität im Schlüsselbund von JUMBO BLOCK CRYPT und tauschen ihre öffentlichen Schlüssel (.jbid) aus.
2. Die Zentrale trägt die Stellen ein, die Stellen legen die Zentrale fest – jeweils mit Abgleich des Fingerabdrucks.
3. Die Stellen liefern ihr Teil-Inventar im vereinbarten Turnus; die Zentrale prüft und übernimmt (Kapitel 10).
4. Die Zentrale verteilt Vorgaben und schickt Änderungen als Rücklieferung zurück (Kapitel 11).

4. Inventar anlegen und öffnen

1. Unter *Neues Inventar* den Namen der Stelle, ein Kurzzeichen und die Organisation eintragen.
2. Passwort mit mindestens 12 Zeichen zweimal eingeben.
3. *Inventar anlegen* klicken und anschließend speichern.

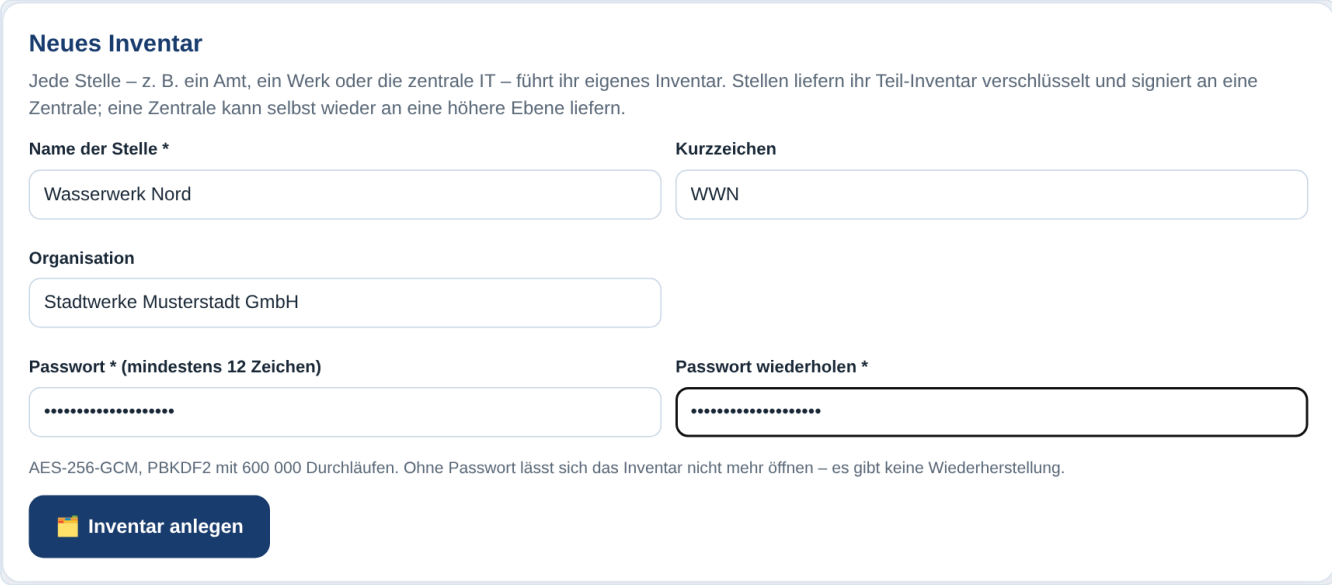


Abb. 2: Neues Inventar anlegen

> Ohne Passwort lässt sich das Inventar nicht mehr öffnen – es gibt keine Wiederherstellung.

- *Inventar öffnen* liest eine vorhandene Datei; danach wird das Passwort abgefragt.
- Das Inventar sperrt sich nach 15 Minuten ohne Eingabe; zum Weiterarbeiten genügt das Passwort.
- Bis zum Speichern wird es zusätzlich verschlüsselt im Browser zwischengespeichert und nach einem Absturz auf der Startseite zur Wiederherstellung angeboten.

Übersicht

Nach dem Öffnen zeigt die Übersicht die Zahl der Objekte, Stelle, Rolle und Prüfwert sowie alle Hinweise und Warnungen.



Abb. 3: Übersicht mit Zahl der Objekte und Prüfwert

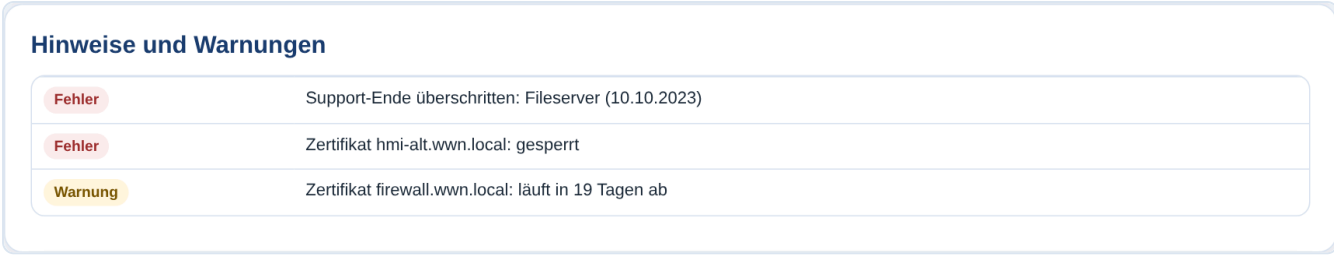


Abb. 4: Hinweise und Warnungen

Prüfung	Beispiel
IP-Adressen	doppelt vergeben, außerhalb aller erfassten Netze, außerhalb der von der Zentrale zugewiesenen Bereiche; Netze überschneiden sich
Geräte	Support-Ende überschritten, Seriennummer mehrfach, ohne Verantwortliche/n, kritisches Gerät ohne Prüfkriterium für den Wiederanlauf
Zertifikate	abgelaufen, gesperrt oder läuft in höchstens 30 Tagen ab
Abhängigkeiten	Verweis auf ein nicht vorhandenes Objekt, zirkuläre Abhängigkeit
Austausch	Lieferung an die Zentrale fällig, Lieferung einer Stelle überfällig, Rücklieferung ausstehend

5. Geräte

Der Reiter *Geräte* listet alle Geräte und Systeme mit Typ, IP-Adressen, Standort, Firmware und Verantwortlichen. Die Suche findet Name, IP-Adresse, Hersteller und Seriennummer; der Typfilter schränkt die Liste ein. Überschrittenes Support-Ende wird mit *EOL* markiert.

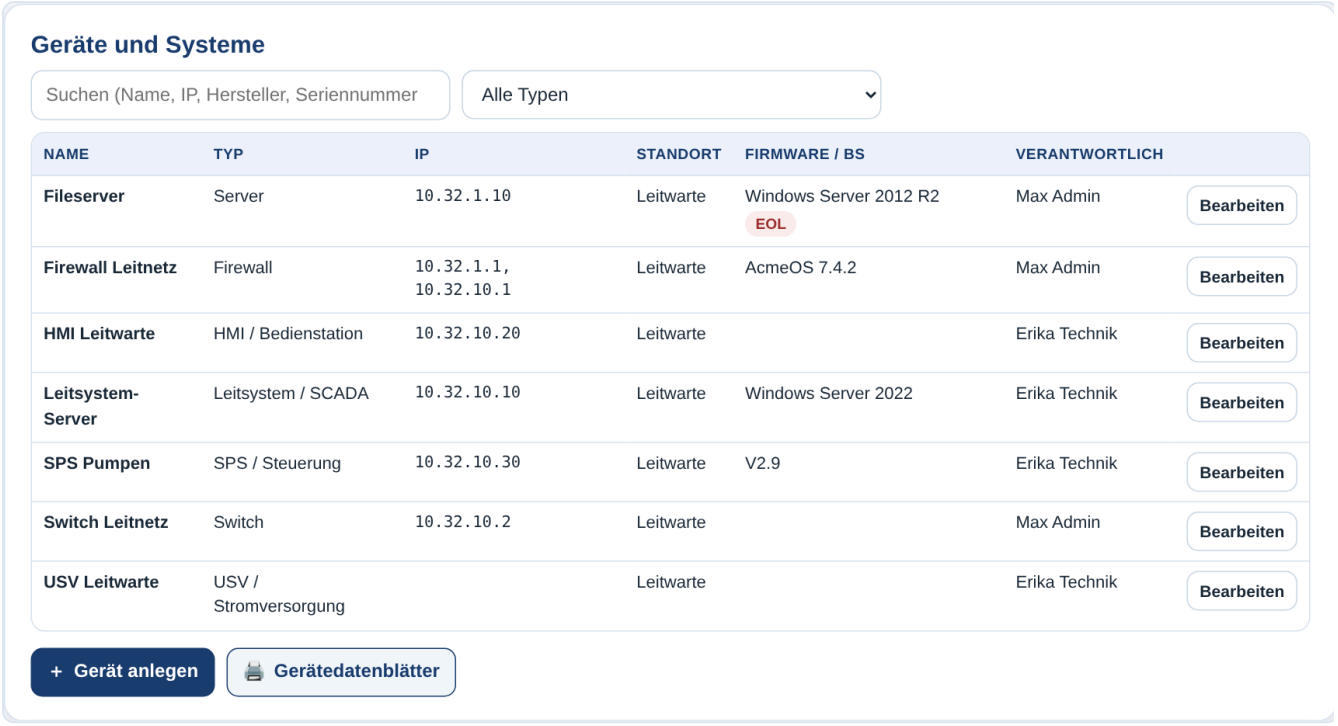


Abb. 5: Geräte eines Wasserwerks

Gerät anlegen oder *Bearbeiten* öffnet das Formular.

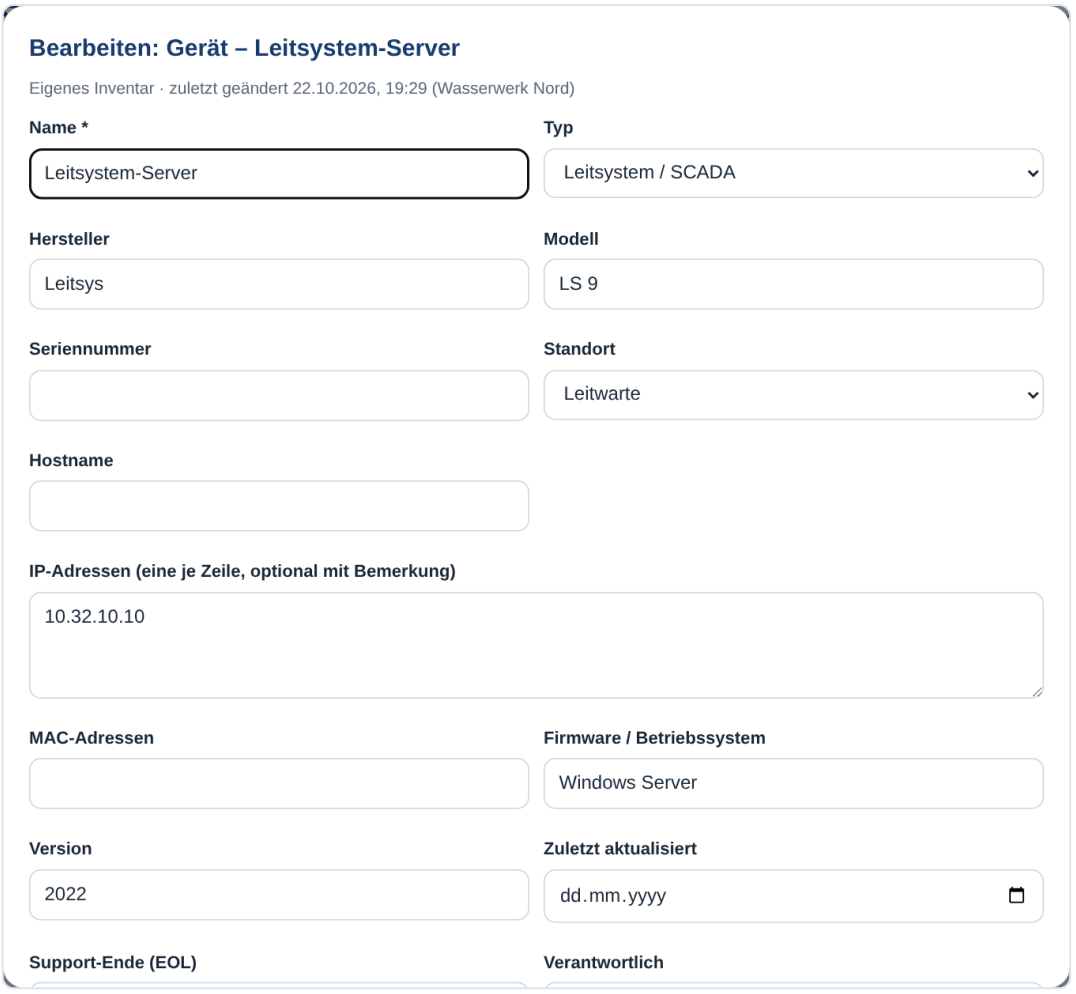


Abb. 6: Formular eines Geräts (Ausschnitt)

Feldgruppe	Felder
Kennzeichnung	Name, Typ (18 Typen von Server über SPS, HMI und Leitsystem bis Feldgerät und USV), Hersteller, Modell, Seriennummer, Standort
Netz	Hostname, IP-Adressen (eine je Zeile, optional mit Bemerkung), MAC-Adressen
Software	Firmware bzw. Betriebssystem, Version, zuletzt aktualisiert, Support-Ende (EOL)
Zuständigkeit	Verantwortlich, Vertretung, Lieferant / Wartung, Wartungsvertrag
Bedeutung	Kritikalität, trägt zu Diensten bei, braucht (Abhängigkeiten)
Zugang	Nur ein Verweis, z. B. auf einen Eintrag in JUMBO BLOCK VAULT – keine Passwörter
Wiederanlauf	Priorität innerhalb der Stufe, Zielzeit, Prüfkriterium „läuft, wenn …“, Schritte bzw. Handbuch

Verweise auf Standorte, Kontakte, Geräte und Dienste werden aus Auswahllisten gewählt; bei *braucht* und *Dienste* ist Mehrfachauswahl mit `Strg` bzw. ⌘ möglich. Ein Objekt, auf das noch verwiesen wird, lässt sich nicht löschen.

Gerätedatenblätter druckt für jedes Gerät ein Blatt mit allen Angaben – für den Notfallordner oder zum Anbringen am Schaltschrank.

Im Feld *Zugang* niemals Passwörter eintragen. Zugangsdaten gehören in einen Passwort-Tresor wie JUMBO BLOCK VAULT.

6. Netze und IP-Plan

Netze werden mit Name, Zone (IT / Büro, OT / Produktion / Leittechnik, DMZ, Management, Gast, Sonstiges), Netz in CIDR-Schreibweise (z. B. `10.32.10.0/24`), VLAN, Gateway, DNS-Servern, DHCP-Bereich, Standort und Verantwortlichen erfasst. Eine Adresse wie `10.32.1.17/24` wird auf die Netzadresse `10.32.1.0/24` korrigiert.

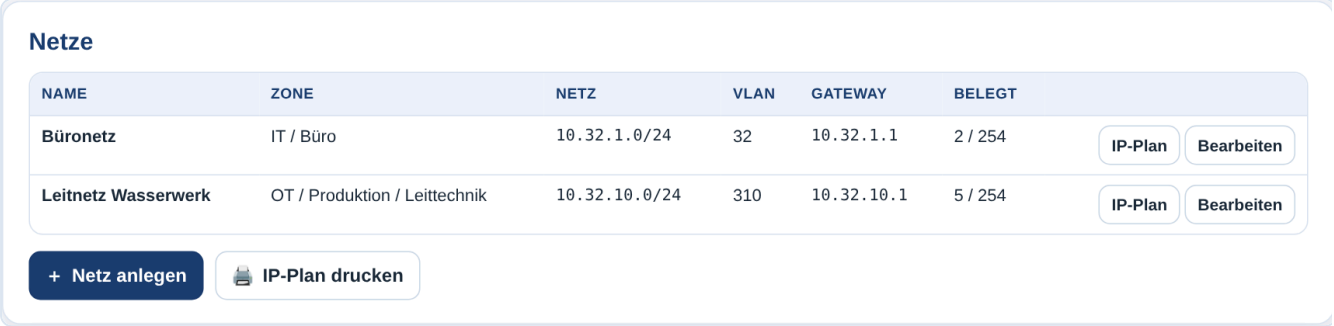


Abb. 7: Netze mit Zone, VLAN, Gateway und Belegung

IP-Plan zeigt für ein Netz alle belegten Adressen mit Gerät, die Zahl belegter und freier Adressen und die freien Bereiche. *IP-Plan drucken* erzeugt den Plan aller Netze zum Ausdrucken.

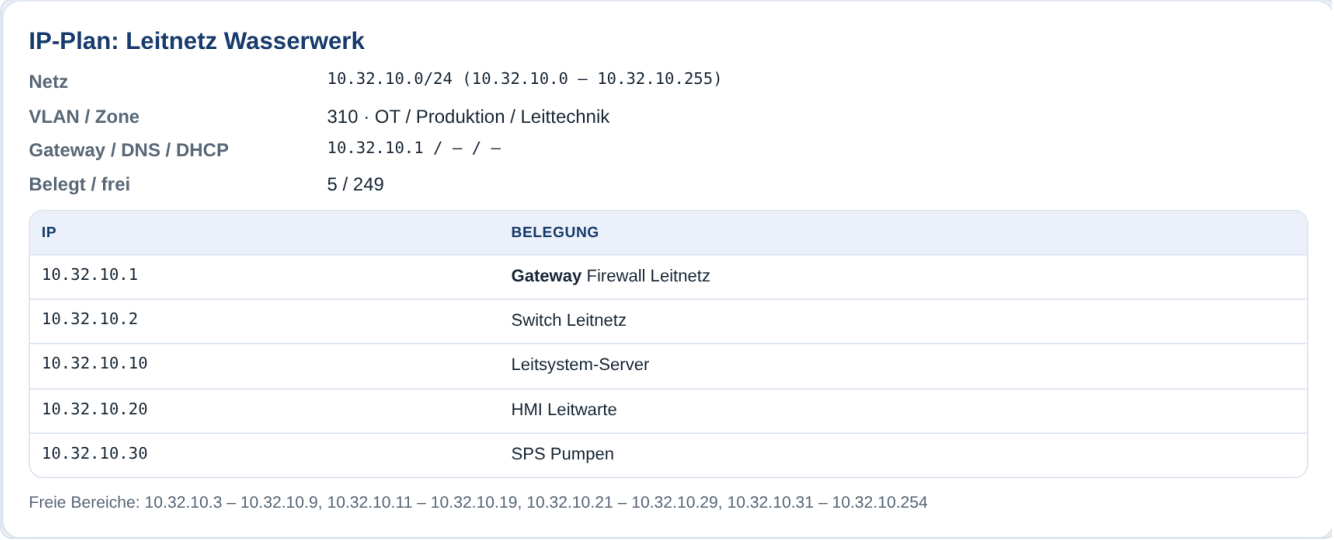


Abb. 8: IP-Plan des Leitnetzes mit Belegung und freien Bereichen

> Doppelt vergebene Adressen und Adressen außerhalb der erfassten Netze erscheinen als Warnung in der Übersicht.

7. Standorte, Kontakte und Dienste

Der Reiter *Standorte, Kontakte, Dienste* fasst die Stammdaten zusammen; der Umschalter wählt die Art.

Art	Felder
Standorte	Name, Art (Gebäude, Raum, Schrank / Rack, Rechenzentrum, Außenanlage), Adresse, liegt in (übergeordneter Standort), Zugang (Schlüssel, Zutritt), Notiz
Kontakte	Name, Art (Person, Dienstleister / Lieferant, Behörde), Funktion, Telefon, Mobil, E-Mail, Erreichbarkeit / Rufbereitschaft, Vertrags- bzw. Kundennummer
Dienste	Kritische Dienstleistung oder Geschäftsprozess mit Beschreibung, Kritikalität, Verantwortlichen, „braucht …“ und Angaben zum Wiederanlauf, z. B. „verfügbar, wenn Druck im Netz > 4 bar“



Abb. 9: Kontakte mit Erreichbarkeit

Notfallkontakte drucken erstellt eine Liste aller Kontakte mit Telefon, Mobil, Erreichbarkeit und den Geräten, Netzen und Diensten, für die sie zuständig sind.

8. Zertifikate

Abgelaufene Zertifikate legen im Ernstfall Bedienoberflächen, Fernwartung und Schnittstellen lahm. INVENTORY führt deshalb alle Zertifikate mit Ablaufdatum und Zuordnung zum Gerät.

- *Register aus CA-Datei (Cert) übernehmen* liest die CA-Datei von JUMBO BLOCK CERT. Nur das Register wird gelesen – ein Passwort ist nicht nötig, der private Schlüssel der CA bleibt verschlüsselt. Bei erneutem Einlesen werden vorhandene Einträge aktualisiert, z. B. gesperrte Zertifikate.
- *Zertifikatsdatei laden (.crt, .pem)* übernimmt einzelne Zertifikate, auch fremder Aussteller.
- *Manuell erfassen* für Zertifikate, deren Datei nicht vorliegt.

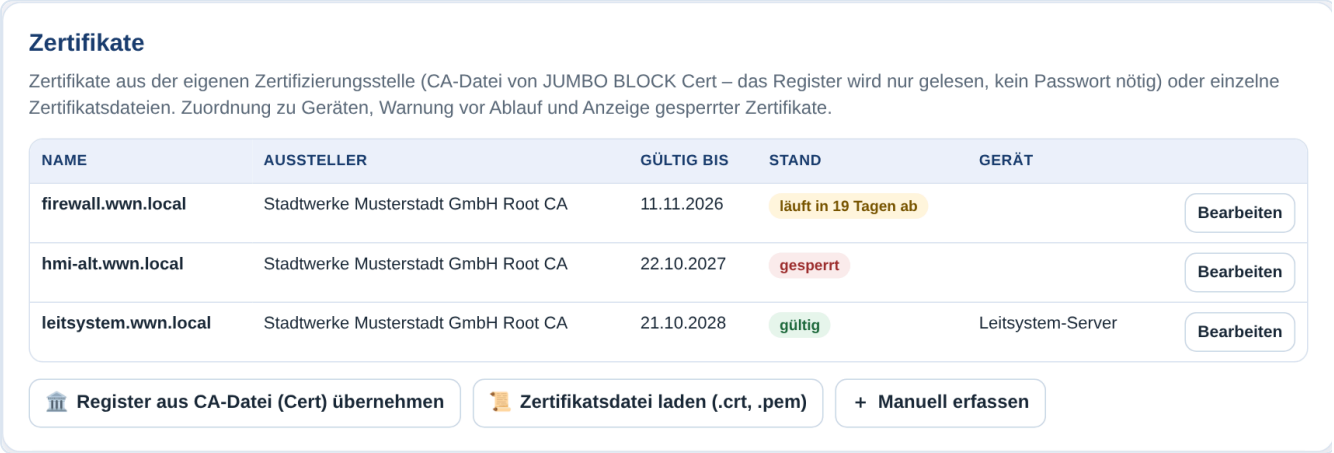


Abb. 10: Zertifikate mit Stand und zugeordnetem Gerät

Die Spalte *Stand* zeigt gültig, läuft in … Tagen ab (ab 30 Tagen vor Ablauf), abgelaufen oder gesperrt. Über *Bearbeiten* wird das Zertifikat einem Gerät zugeordnet.

9. Wiederanlauf

Aus den Angaben „braucht …“ aller Geräte und Dienste berechnet INVENTORY die Wiederanlaufreihenfolge in Stufen: Stufe 1 enthält alles, was nichts anderes braucht, Stufe 2 alles, was nur Stufe 1 braucht, und so weiter. Innerhalb einer Stufe entscheidet die Priorität.

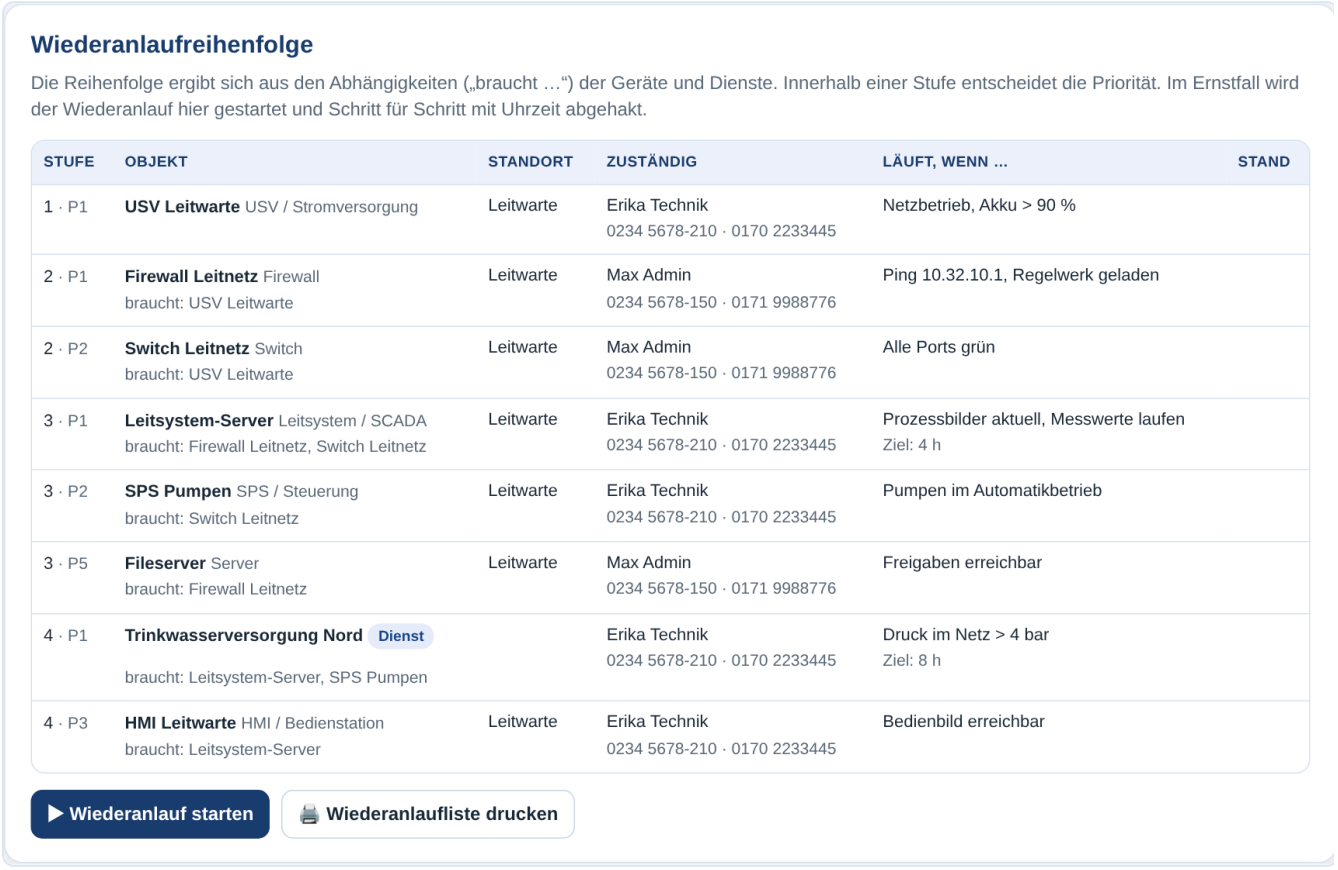


Abb. 11: Wiederanlaufreihenfolge mit Stufen, Zuständigen und Prüfkriterien

Für jedes Objekt stehen Standort, Zuständige mit Telefon und das Prüfkriterium „läuft, wenn …“ mit Zielzeit in der Liste. Eine zirkuläre Abhängigkeit wird gemeldet, weil sich dann keine Reihenfolge bestimmen lässt. *Wiederanlaufliste drucken* erzeugt eine Liste zum Abhaken mit Spalte für Uhrzeit und Kürzel.

Im Ernstfall

1. *Wiederanlauf starten* – Anlass und Leitung angeben.
2. Für jedes Objekt den Stand setzen: ▶️ wird hochgefahren, ✅ läuft, ⚠️ Problem (mit Notiz). Die Uhrzeit wird festgehalten. Objekte, deren Voraussetzungen noch nicht laufen, zeigen „wartet auf …“.
3. Mit *Stand an das Lagebuch melden* den aktuellen Stand als verschlüsselte Meldung an JUMBO BLOCK LOGBOOK schicken – dafür einmal den Meldeschlüssel (.jbk) des Lagebuchs laden.
4. Nach Abschluss *Wiederanlauf beenden*.

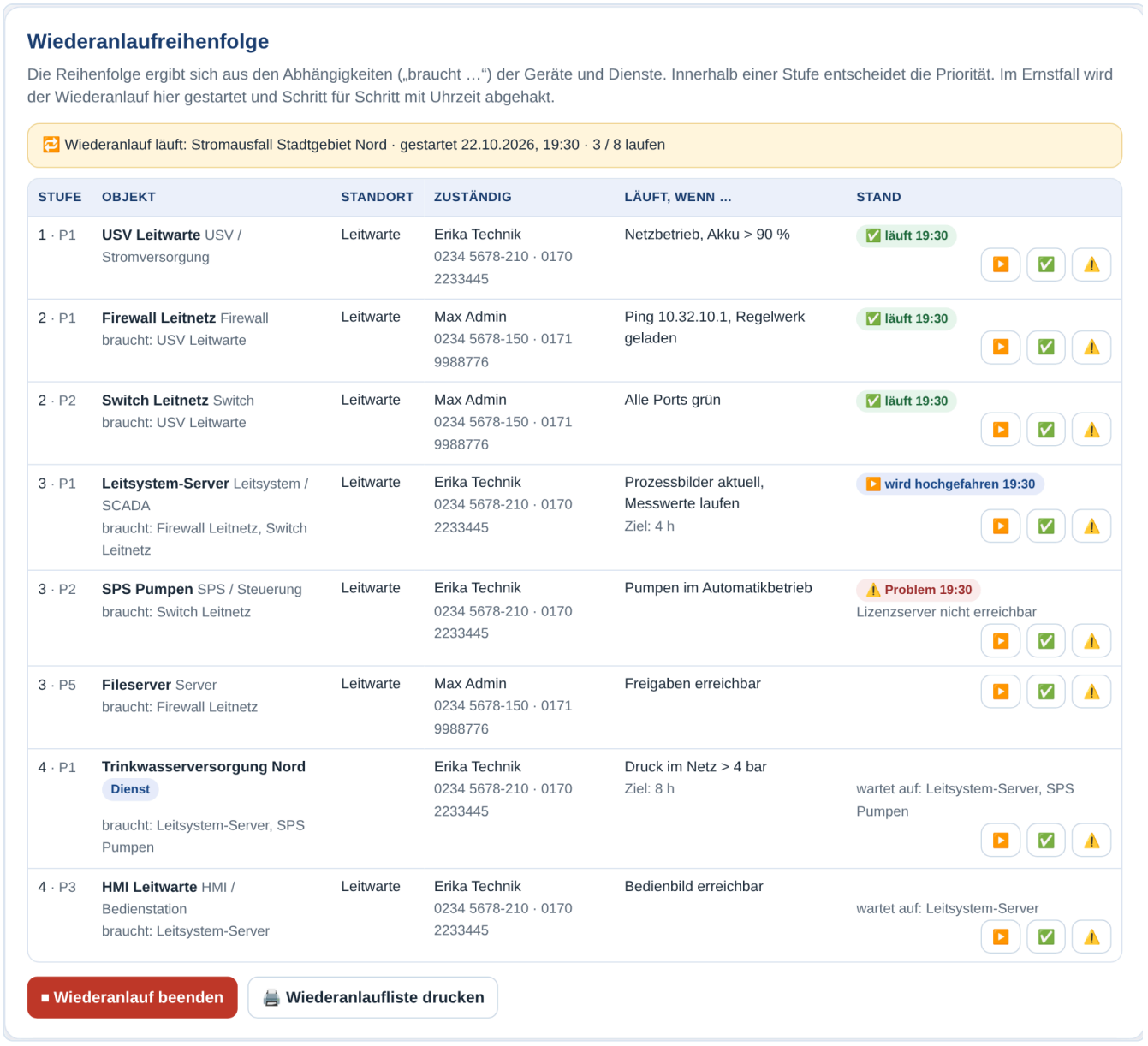


Abb. 12: Laufender Wiederanlauf mit Stand je Objekt



Abb. 13: Meldung an das Lagebuch

Start, jeder Statuswechsel, Meldungen an das Lagebuch und das Ende werden in der Prüfkette festgehalten.

10. Lieferung an die Zentrale

Lieferungen werden mit einer Identität aus dem Schlüsselbund von JUMBO BLOCK CRYPT verschlüsselt und signiert. Der Schlüsselbund wird im Reiter *Austausch* mit *Schlüsselbund öffnen …* geladen; er bleibt nur bis zum Sperren geöffnet und wird nicht verändert.

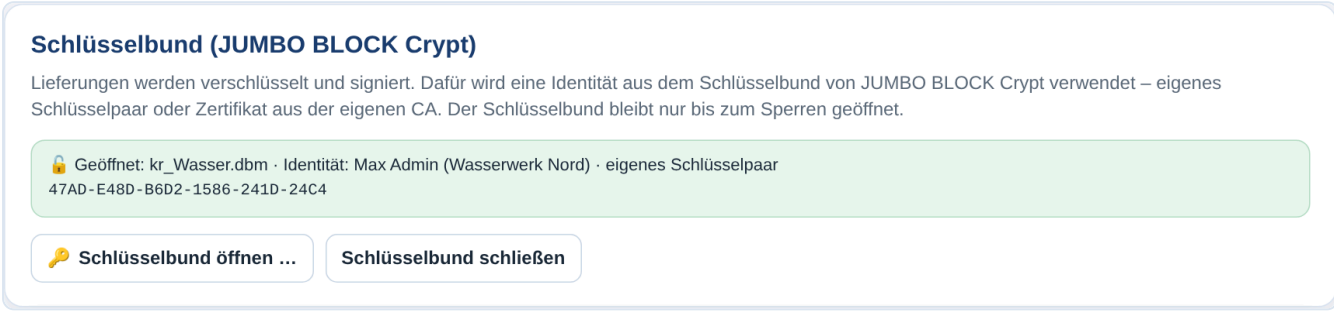


Abb. 14: Geöffneter Schlüsselbund mit gewählter Identität

Zentrale festlegen

Zentrale festlegen (.jbid) … lädt den öffentlichen Schlüssel der Zentrale. Gleichen Sie den Fingerabdruck mit der Zentrale ab – telefonisch oder persönlich. Nur Pakete mit genau diesem Schlüssel werden danach als Rücklieferung oder Vorgaben angenommen.

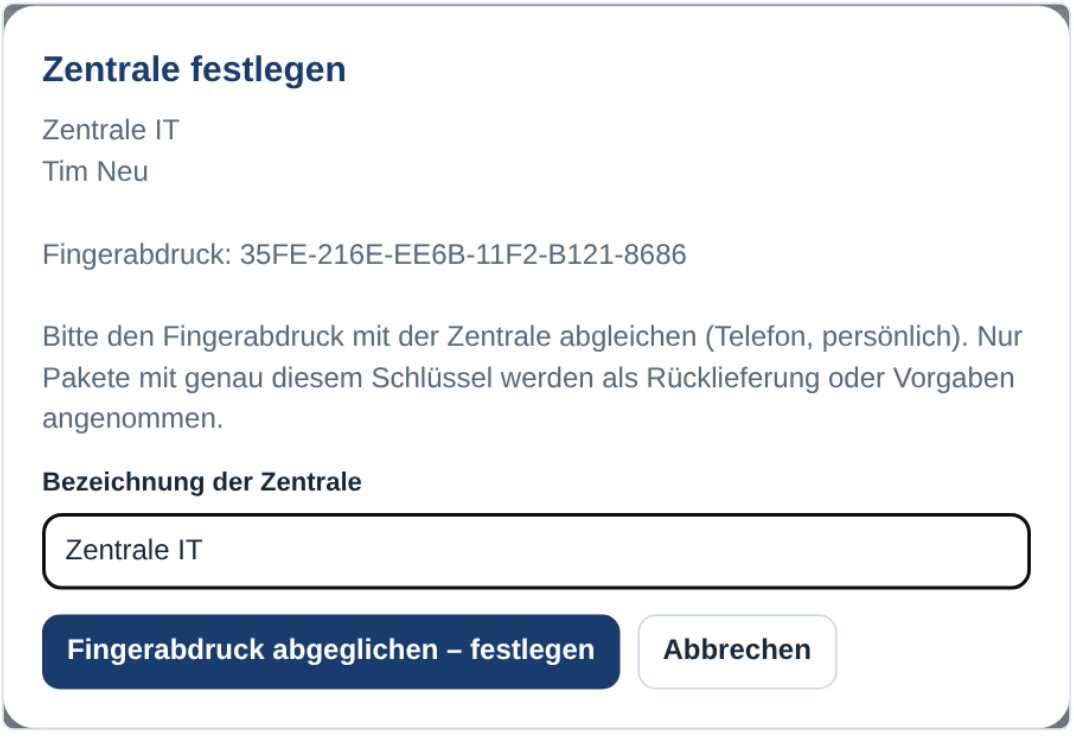


Abb. 15: Zentrale festlegen mit Abgleich des Fingerabdrucks

Lieferung erstellen

Der Bereich *An die Zentrale liefern* zeigt Zentrale, letzten Lieferstand und die Zahl der Änderungen seit der letzten Lieferung. *Lieferung erstellen* erzeugt das Paket (.jbc), das Sie der Zentrale übergeben. *Eigenen*

öffentlichen Schlüssel (.jbid) speichert den Schlüssel, den die Zentrale zum Eintragen der Stelle braucht.



Abb. 16: An die Zentrale liefern

Gibt die Zentrale einen Lieferturnus vor, weist die Übersicht auf eine fällige Lieferung hin.

11. Zentrale: Stellen zusammenführen

Stellen eintragen

- *Stelle hinzufügen (.jbid)* lädt den öffentlichen Schlüssel einer Stelle. Nach dem Abgleich des Fingerabdrucks wird sie mit einer Bezeichnung eingetragen. Nur Lieferungen mit genau diesem Schlüssel werden ihr zugeordnet.
- *Stelle ohne Inventory (CSV)* übernimmt die Liste einer Stelle, die INVENTORY nicht selbst nutzt.

Lieferungen empfangen

Paket einlesen (.jbc) erkennt die Art des Pakets, prüft Verschlüsselung, Signatur, Absender und Anschluss an den letzten Stand und zeigt alle Änderungen gegenüber dem bisherigen Stand.

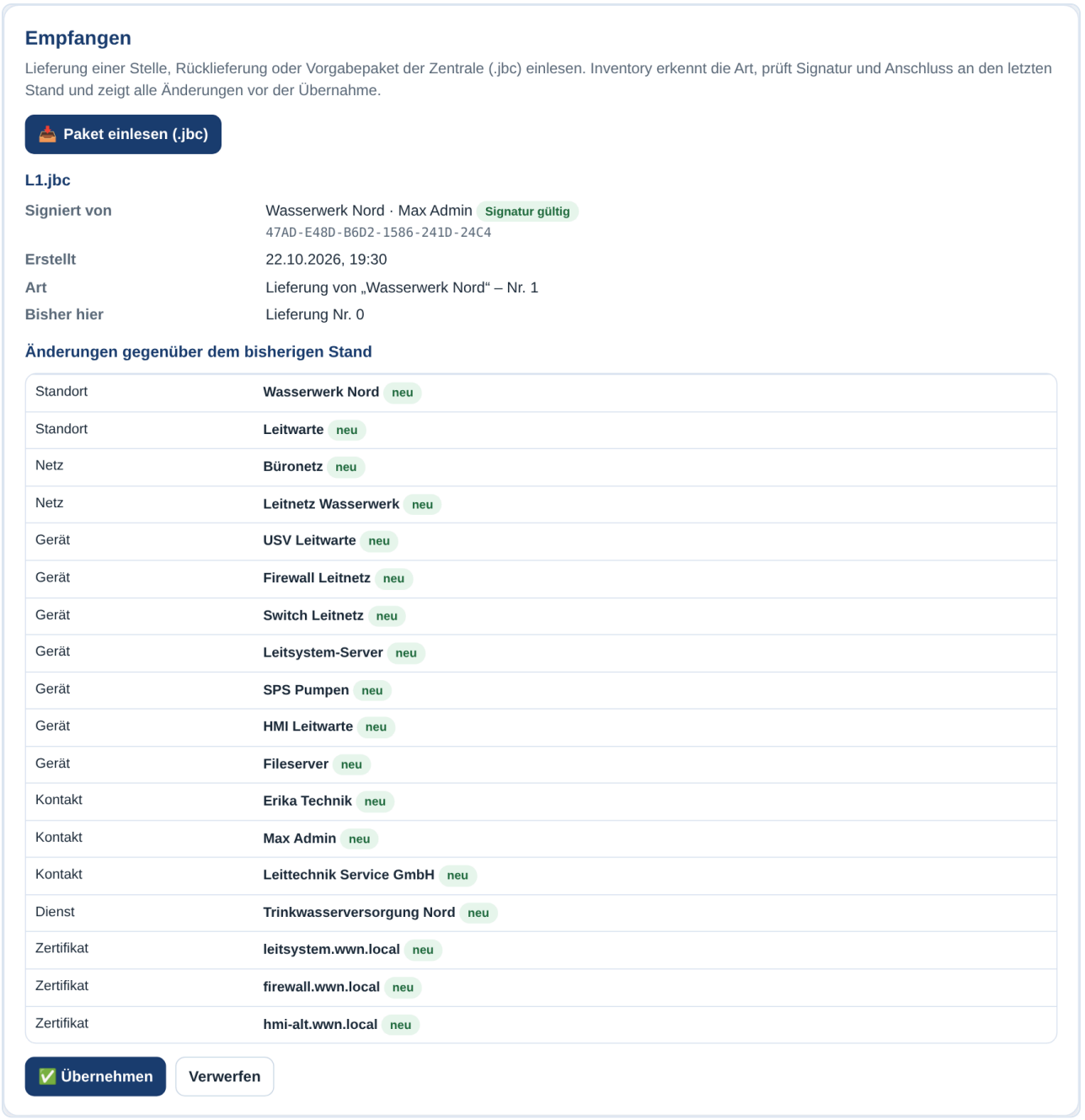


Abb. 17: Lieferung einer Stelle mit Änderungen

Übernehmen führt das Teil-Inventar in das Gesamtinventar; *Verwerfen* lehnt die Lieferung ab. Beides wird protokolliert. Lieferungen fremder Absender, veränderte oder unsignierte Pakete und ältere Stände werden abgelehnt.



Abb. 18: Untergeordnete Stellen mit Lieferstand

Ansicht wählen

Über *Ansicht* wechselt die Zentrale zwischen dem eigenen Inventar, der *Gesamtsicht (alle Stellen)* zum Lesen und dem Teil-Inventar einer einzelnen Stelle. In der Gesamtsicht trägt jedes Objekt die Bezeichnung seiner Stelle.

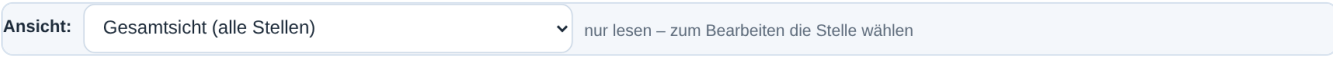


Abb. 19: Auswahl der Ansicht

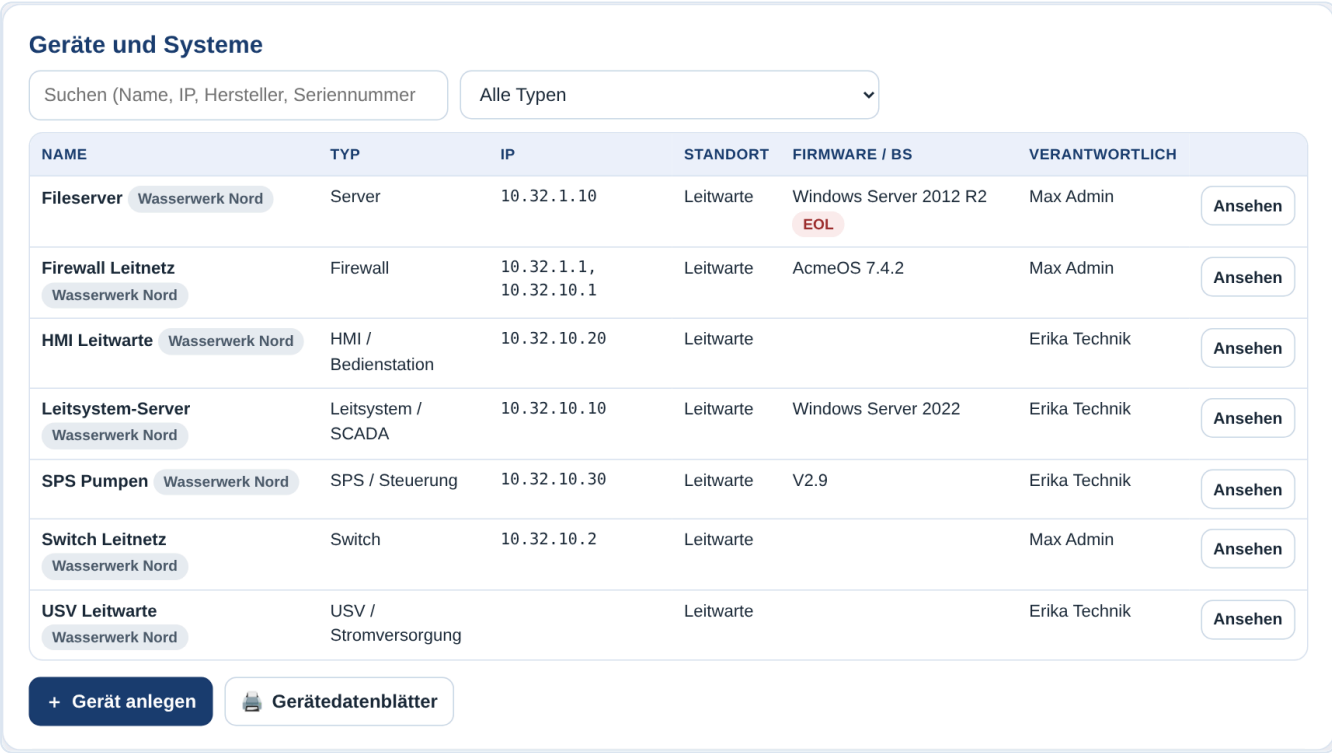


Abb. 20: Gesamtsicht der Geräte aller Stellen

Daten einer Stelle ändern und Rücklieferung

Die Zentrale darf Datensätze einer Stelle ändern. Diese Änderungen müssen als **Rücklieferung** an die Stelle gehen: Bis die Stelle sie eingespielt hat, nimmt die Zentrale von dieser Stelle keine Lieferung auf älterem Stand an. Bei der Stelle ersetzt die Rücklieferung das bisherige Teil-Inventar vollständig. Eigene

Änderungen, die die Stelle seit ihrer letzten Lieferung gemacht hat, bietet INVENTORY danach einzeln zum erneuten Anwenden an – ohne Konflikt vorausgewählt, bei Konflikten entscheidet die Stelle bewusst.

12. Vorgaben der Zentrale

Vorgabepaket erstellen … erzeugt ein Paket für alle eingetragenen Stellen. Es enthält die Standorte, Netze, Geräte, Kontakte und Dienste der Zentrale (ohne Zertifikate), die jeder Stelle zugewiesenen IP-Bereiche und den Lieferturnus in Tagen.



Abb. 21: Vorgabepaket mit Lieferturnus und zugewiesenen IP-Bereichen

Bei der Stelle wird das Paket über *Paket einlesen* eingespielt. Die Vorgaben erscheinen grau und nur lesend, z. B. zentrale DNS-Server oder Ansprechpartner der zentralen IT. Eigene Objekte können auf sie verweisen. IP-Adressen außerhalb der zugewiesenen Bereiche werden als Warnung angezeigt.

Ein Vorgabepaket wird nur angenommen, wenn es von der festgelegten Zentrale signiert ist und einen neueren Stand trägt. Ist noch keine Zentrale festgelegt, legt das Einspielen den Absender als Zentrale fest – vorher den Fingerabdruck abgleichen.



Abb. 22: Gesamtsicht der Zentrale

13. Datei, CSV und Prüfkette

Inventardatei



Abb. 23: Inventardatei

Schaltfläche	Wirkung
Speichern / Speichern unter …	Speichert verschlüsselt; in Chrome und Edge mit *Automatisch speichern* nach jeder Änderung
Sperren · Passwort ändern · Schließen	Wie in den anderen Programmen der Suite
Angaben zur Stelle	Name, Kurzzeichen und Organisation der Stelle ändern

CSV-Import und -Export

Vorhandene Listen, z. B. aus Excel, lassen sich übernehmen. Art wählen, *CSV exportieren* liefert eine Vorlage mit den Spaltennamen. Beim Import muss die erste Zeile Spaltennamen wie in der Exportdatei enthalten; Trennzeichen Semikolon oder Komma. Verweise auf Standorte und Kontakte werden über den Namen zugeordnet und fehlende automatisch angelegt. Nicht zugeordnete Spalten werden gemeldet.



Abb. 24: CSV-Import und -Export

Prüfkette

Jede Änderung an Objekten, jeder Austausch und jeder Wiederanlauf wird mit Zeitpunkt und SHA-256-Hash festgehalten. Die Prüfkette sichert zusätzlich den Datenstand jeder Ansicht. Beim Öffnen prüft INVENTORY, ob Kette und Daten zusammenpassen.

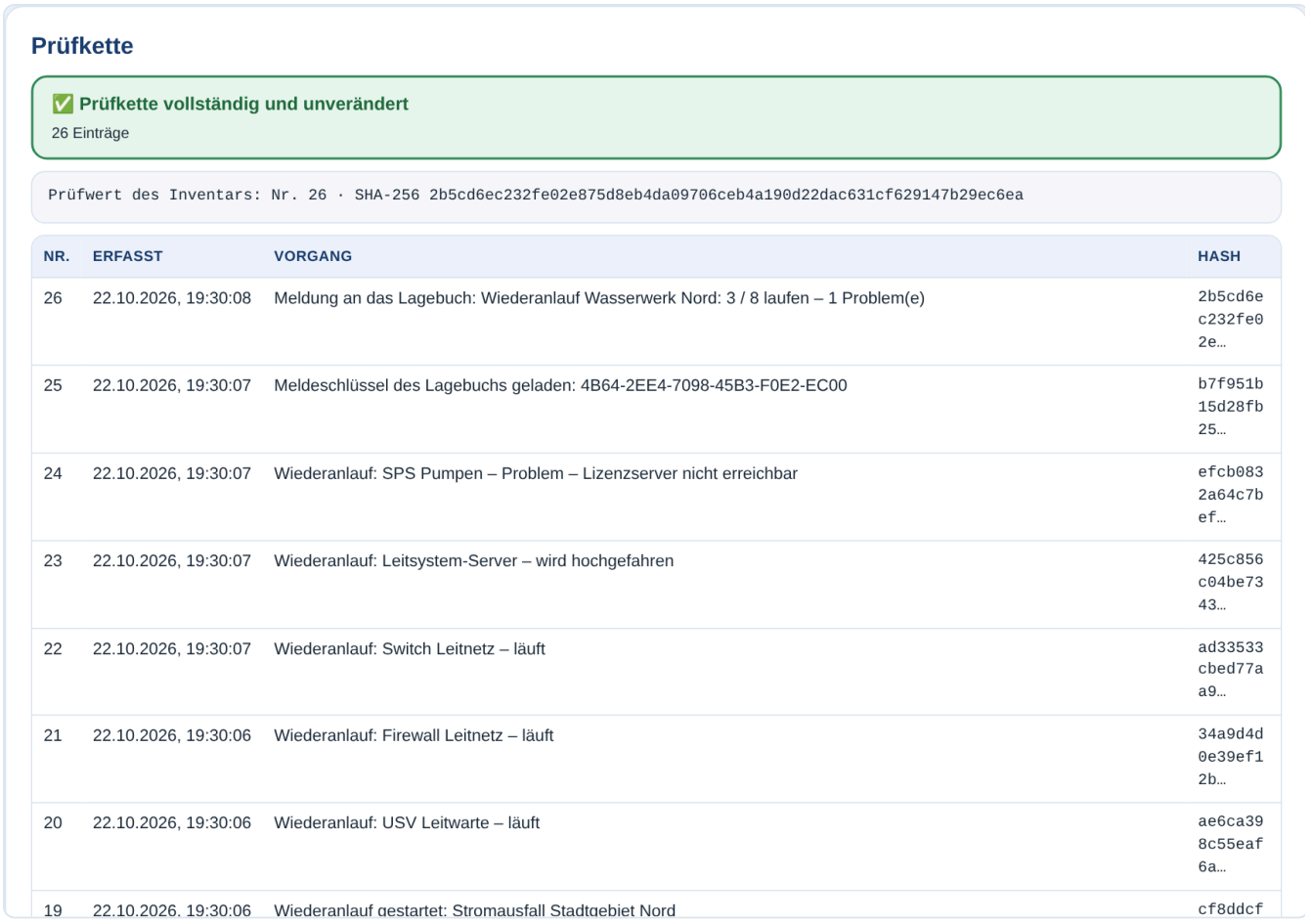


Abb. 25: Prüfkette

14. Sicherheit und Technik

Bereich	Umsetzung
Inventardatei	AES-256-GCM, PBKDF2-SHA-256 mit 600 000 Durchläufen; zusätzliche SHA-256-Prüfsumme der Datei
Pakete	Dateiformat von JUMBO BLOCK CRYPT (.jbc): ECDH P-256, HKDF-SHA-256 und AES-256-GCM für die Empfänger, Signatur des Absenders mit ECDSA oder RSA
Zuordnung	Stellen und Zentrale werden über den Fingerabdruck ihres Schlüssels erkannt; Lieferstände über Laufnummern und Prüfsummen
Prüfkette	SHA-256 je Eintrag mit Vorgänger-Hash, beginnend mit „GENESIS“, mit Hash des Datenstands
Meldungen	Wiederanlauf-Meldungen im Format von JUMBO BLOCK LOGBOOK, verschlüsselt mit dem Meldeschlüssel des Lagebuchs
Datenschutz	Keine Netzwerkverbindung, keine Telemetrie; keine Passwörter im Inventar

Grenzen

- INVENTORY sucht nicht selbst im Netz nach Geräten. Die Angaben sind so gut wie ihre Pflege – regelmäßig prüfen und liefern.
- Das Inventar ist eine sensible Datei: Es beschreibt Netze, Adressen und Zuständigkeiten. Ausdrucke wie Zugangsdaten behandeln.
- Gleichzeitiges Arbeiten mehrerer Personen in derselben Datei ist nicht vorgesehen; dafür sind Stellen und Lieferungen da.

15. Fehlerbehebung

Problem	Ursache und Lösung
„Das Netz bitte in CIDR-Schreibweise angeben“	Netz als Adresse mit Präfix eingeben, z. B. `10.20.1.0/24`.
„Wird noch verwendet von …“ beim Löschen	Erst die Verweise in den genannten Objekten entfernen.
„Zirkuläre Abhängigkeit im Wiederanlauf“	Zwei Objekte brauchen sich gegenseitig. Eine der Abhängigkeiten entfernen.
„Das Paket ist nicht für eine Identität dieses Schlüsselbunds verschlüsselt“	Falscher Schlüsselbund geöffnet oder Paket für eine andere Stelle. Richtigen Schlüsselbund öffnen.
„Der Absender ist nicht als untergeordnete Stelle eingetragen“	Die Stelle zuerst mit ihrem öffentlichen Schlüssel (.jbid) eintragen.
Lieferung abgelehnt wegen nicht verschickter Änderungen der Zentrale	Zuerst die Rücklieferung erstellen oder die Änderungen verwerfen; danach liefert die Stelle auf neuem Stand.
„Dieses Vorgabepaket ist bereits eingespielt oder veraltet“	Ein neueres Vorgabepaket ist bereits eingespielt. Kein Handlungsbedarf.
CSV-Import: „Keine Spalte Name gefunden“	Erste Zeile muss die Spaltennamen enthalten; Vorlage per *CSV exportieren* erzeugen.
„Prüfkette verletzt“	Die Datei wurde außerhalb von INVENTORY verändert. Sicherung vergleichen.