LocalEye Admin Manual

Installation, Betrieb und Störungsbehebung für Administratoren

---

Stand 24.11.2026, ab Version 2026.11.24-1045

Inhalt

1. Für wen dieses Handbuch ist

2. Aufbau in Kürze

3. Voraussetzungen

4. Installation

5. Erste Einrichtung

6. Lizenz

7. Datenschutzprofil

8. Benutzer, Rechte und Anmeldung

9. Kameras und NVR

10. KI, Zonen und Prüfhinweise

11. Meldungen

12. Fernzugriff

13. Aufnahmen, Fristen und Nachweise

14. Updates

15. Sicherung und Wiederherstellung

16. Überwachung und Diagnose

17. Verbund und Leitstelle

18. Störungen beheben

19. Referenz

1. Für wen dieses Handbuch ist

Dieses Handbuch richtet sich an Administratoren und Techniker, die eine LocalEye-Anlage einrichten und betreiben. Es beschreibt den Stand vom 16.11.2026, ab Version 2026.11.16, und führt von der Installation bis zur Störungsbehebung.

Für die tägliche Bedienung gibt es das Anwender-Handbuch. Aufbau, Datenflüsse und Sicherheitskonzept stehen im IT-Security- und Architektur-Konzept.

Zeichen in diesem Handbuch

> Blaue Kästen geben Hinweise.

> Rote Kästen warnen vor Datenverlust oder Sicherheitsrisiken.

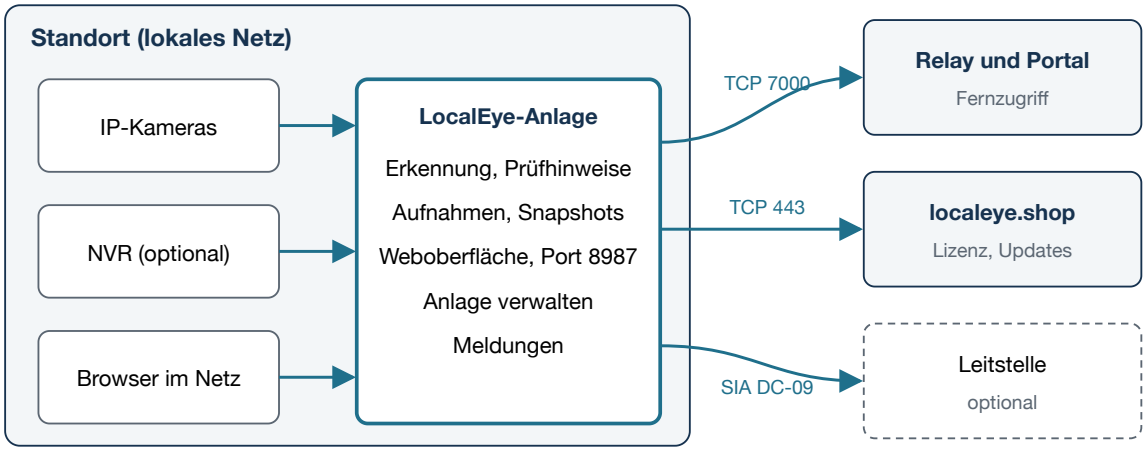
> Grüne Kästen enthalten Empfehlungen.

Begriffe

Begriff	Bedeutung
Anlage	Das LocalEye-Gerät am Standort
Anlage verwalten	Verwaltungsoberfläche unter `/anlage/`, nur im lokalen Netz erreichbar
Hauptanlage	Vollständige Anlage mit Oberfläche und Lizenzschlüssel
Kamera-Erweiterung	Zusatzgerät im Verbund für Kameras, Aufnahme und KI, ohne eigene Oberfläche
Portal	Anmeldeseite für den Fernzugriff unter `remote.localeye.shop`
Prüfhinweis	Verdachtsmoment der KI zur menschlichen Prüfung, keine Feststellung
Griff-Wache	Meldet mögliches Einstecken von Ware als Prüfhinweis, siehe Kapitel Griff-Wache
Leitstelle (Rolle)	Konto für den Prüfzugang der Alarm-Leitstelle unter `/leitstelle/`, siehe Kapitel Verbund und Leitstelle
Datenschutzprofil	Schalter für strenge Vorgaben, siehe Kapitel Datenschutzprofil
EDEKA-Betrieb	Datenschutzprofil mit Profilsperre und den Voreinstellungen aus `.env.edeka.example`

2. Aufbau in Kürze

Die Anlage ist ein Linux-Rechner mit Docker. Kameras liefern ihre Streams im lokalen Netz an die Anlage. Erkennung, Bildbeschreibung und Speicherung laufen dort. Die Anlage arbeitet im Betrieb eigenständig und braucht dafür weder Relay noch Shop.



Alle Verbindungen nach außen baut die Anlage von innen auf. Im Router wird kein Port geöffnet.

Dienste auf der Anlage

Dienst	Aufgabe
nginx	Einziger Eingang, Port 8987
LocalEye	Erkennung, Aufnahmen, Oberfläche, Rechte, Meldungen
go2rtc	Stream-Dienst für Kameras
Bild-KI	Lokale Bildbeschreibung für Prüfhinweise
ntfy	Eigener Push-Dienst
Anlage verwalten	Lizenz, Update, Sicherung, Betrieb
Fernzugriff	Ausgehende Verbindung zum Relay

3. Voraussetzungen

Hardware

Kameras	Gerät	Ergebnis
bis 32, 4 MP mit Unterstrom	6 Threads, 32 GB, ohne GPU	Erkennungstakt vollständig gehalten, CPU 79 %
48, 4 MP mit Unterstrom	6 Threads, 32 GB, ohne GPU	an der Grenze, CPU 95 %
16, nur Hauptstrom 4 MP	6 Threads, 32 GB, ohne GPU	Erkennungstakt gehalten, CPU 70 %

Gemessen am 05.11.2026 mit echten, getrennten Strömen von 4-MP-Kameras, Erkennung alle 5 Sekunden, Bildbeschreibung auf der CPU, mit dem Stand, der in Version 2026.11.09 enthalten ist. Für 45 bis 50 Kameras mehr Kerne oder eine GPU einplanen und die Werte auf der Zielhardware messen. Speicher als Richtwert: rund 0,2 bis 0,3 TB je Kamera bei Daueraufzeichnung über 15 Tage, LocalEye selbst zeichnet nur Ereignisse auf. Ohne GPU läuft die Bildbeschreibung für Prüfhinweise nur stichprobenhaft.

Software

- Linux-Server mit aktuellem Docker und dem Plugin `docker compose`
- Python 3, `curl` und `rsync` für `manage.sh`
- Mindestens 60 GB freier Speicher zusätzlich zu den Aufnahmen
- Zeitsynchronisation per NTP, sie ist für 2FA-Codes und den Verbund nötig

Firewall

Richtung	Ziel	Zweck
ausgehend	`remote.localeye.shop`, TCP 7000	Fernzugriff, entfällt wenn abgeschaltet
ausgehend	`localeye.shop`, TCP 443	Lizenz, Updates, Rückfall für KI-Modelle
ausgehend	Docker-Registries einschließlich ghcr.io, PyPI, npm-Registry, GitHub, Hugging Face, Debian-, Alpine- und NodeSource-Paketquellen, optional download.swift.org. TCP 443, Paketquellen teils TCP 80	Bei Installation und Update, auch für abgeschaltete Zusatz-Apps
ausgehend	Mailserver, TCP 587 oder 465	Meldungen per E-Mail
ausgehend	`ntfy.sh`, TCP 443	iOS-Wecksignal, im Datenschutzprofil aus
ausgehend	Leitstelle nach deren Vorgabe	Optional
lokal	Kameras und NVR: RTSP 554, ONVIF und ISAPI meist 80, SADP UDP 37020	Kamera-Anbindung

Richtung	Ziel	Zweck
eingehend aus dem Internet	keine	Im Router wird nichts freigegeben
eingehend aus dem lokalen Netz	Weboberfläche, Medien- und Push-Dienst	Bedienung
eingehend aus dem VPN der Leitstelle	Weboberfläche, z. B. `https://<IP>:8943/leitstelle/`	Optional, Prüfzugang der Leitstelle

> TCP 7000 muss von SSL-Inspection ausgenommen sein. Die Anlage prüft das Zertifikat des Relays immer und verbindet sich bei aufgebrochenem TLS nicht.

> Ein eigenes Kamera-VLAN wird empfohlen. Die Weboberfläche läuft im lokalen Netz ab Werk über HTTP und zusätzlich über HTTPS, siehe „HTTPS im Marktnetz“. Ohne `LAN_HTTP=aus` gehört die Anlage deshalb in ein abgetrenntes Netz.

4. Installation

1. Ordner anlegen, zum Beispiel `/opt/allinone-wl`, und dorthin wechseln.
2. `allinone_whitelabel_release.zip` in diesen Ordner legen.
3. `python3 -c "import zipfile; zipfile.ZipFile('allinone_whitelabel_release.zip').extract('manage.sh')"`
4. `chmod +x manage.sh`
5. `./manage.sh update`

Das Skript entpackt die ZIP, legt Konfiguration und Geheimnisse an, sucht freie Ports und startet die Verwaltungsoberfläche noch vor der Lizenzprüfung. Sobald ein Lizenzschlüssel vorliegt, baut die Anlage ihre Images und startet alle Dienste. Der erste Bau dauert je nach Leitung und Rechner länger.

> Beim ersten Lauf im Terminal fragt das Skript nach der Betriebsart, Hauptstandort ist der Normalfall. Danach fragt es nach dem Lizenzschlüssel. Bleibt die Eingabe leer, endet der Lauf mit einem Fehler, und die Einrichtung geht im Browser weiter. Eine Kamera-Erweiterung braucht keinen Schlüssel, sondern die Adresse der Hauptanlage.

Einrichtung im Browser

Es gibt kein Standardpasswort.

1. `http://<IP>:8987/` öffnen, die Seite führt zu „Anlage verwalten“.
2. Aus dem Netz verlangt die Seite den **Einrichtungscode**. Er steht am Ende der Ausgabe von `./manage.sh update`, `./manage.sh config` erzeugt einen neuen. Am Gerät selbst ist kein Code nötig.
3. Lizenzschlüssel eintragen. Er ist der Schlüssel aus der Bestellbestätigung, nicht die Bestellnummer.
4. Ersten Admin mit eigenem Namen und Passwort anlegen, mindestens 8 Zeichen.
5. Zweiten Faktor einrichten: QR-Code mit einer Authenticator-App scannen, Code eingeben und die acht Wiederherstellungs-Codes sicher ablegen. Ohne diesen Schritt lässt sich die Einrichtung nicht abschließen.
6. Einrichtung abschließen und mit diesem Konto in LocalEye anmelden. Für die erste Anmeldung nach dem Einrichten gilt der nächste Code der App, nicht der eben zur Bestätigung eingegebene.

> Mit abgeschlossener Einrichtung startet der Fernzugriff von selbst, wenn er nicht abgeschaltet ist. Soll er aus bleiben, schalten Sie ihn in „Anlage verwalten“ ab.

Betrieb ohne zweites Gerät

Am angeschlossenen Monitor zeigt `sudo ./manage.sh webgui on` die Oberfläche im Vollbild. Per SSH öffnet `./manage.sh webgui` sie im Terminal, `./manage.sh webgui tunnel` gibt den Befehl für einen SSH-Tunnel aus.

EDEKA-Betrieb

Die Release-ZIP enthält die Vorlage `.env.edeka.example`. Die Anlage liest sie nicht selbst, `./manage.sh profil edeka` überträgt sie in die `.env`.

1. Nach dem ersten `./manage.sh update`, bevor der Lizenzschlüssel eingetragen wird, `./manage.sh profil edeka` am Terminal ausführen. Der Befehl fragt nach dem Markt-LAN für `VERWALTUNG_LAN_CIDRS` und schlägt das Netz der eigenen Schnittstelle vor. Danach von Hand in die `.env` eintragen: `PRIVACY_SMTP_HOSTS` für den Mailserver des Markts, für den Prüfzugang der Leitstelle `LEITSTELLE_CIDRS` und bei Bedarf `LEITSTELLE_FENSTER_MIN`, für eine andere Frist der Sicherungen `SICHERUNG_FRIST_TAGE`. So startet der Fernzugriff nie, und die Voreinstellung gilt ab dem ersten Start.
2. Die Einrichtung im Browser über `http://<IP>:8987/` abschließen, zweiter Faktor eingeschlossen.
3. `./manage.sh profil edeka` noch einmal ausführen. Erst jetzt setzt der Befehl `LAN_HTTP=aus` und startet die Anlage mit Neubau neu: Den HTTPS-Zugang richtet LocalEye bei seinem ersten Start ein, vorher wäre die Anlage aus dem Netz gar nicht erreichbar. Der Befehl setzt den Wert deshalb nur, wenn die Einrichtung abgeschlossen ist und HTTPS antwortet. Ab dann gilt `https://<IP>:8943/`.
4. Sicherungs-Passwort setzen, bevor die erste Sicherung entsteht: „Anlage verwalten“, Karte Sichern, „Sicherungs-Passwort“, oder `sudo ./manage.sh sicherung-passwort`. Im Datenschutzprofil entsteht ohne Passwort keine Sicherung, siehe Kapitel Sicherung und Wiederherstellung.
5. Soll die Leitstelle Alarme auf der Anlage prüfen: ein Konto mit der Rolle „Leitstelle“ anlegen und an ihren SIA-Kanal binden, siehe Kapitel Verbund und Leitstelle, „Prüfzugang der Leitstelle“.
6. Freigaben mit Begründung und Enddatum erteilen, siehe Kapitel Datenschutzprofil; eine Freigabe ohne Ende meldet die Abnahme als ABWEICHUNG. Dann prüfen mit `./manage.sh selbsttest` und `sudo ./manage.sh abnahme`, siehe unten.

Was `./manage.sh profil edeka` überträgt: nur `PRIVACY_PROFILE`, `PRIVACY_LOCK`, `FERNZUGRIFF`, `COMPOSE_PROFILES` samt den Abwahl-Zeilen der Zusatz-Apps und, nach der Einrichtung, `LAN_HTTP`. Ein gesetztes `GO2RTC_BIND_OPEN` kommentiert er aus. Ports, Lizenz, Schlüssel, Mailserver (`PRIVACY_SMTP_HOSTS`), ein gültiges Markt-LAN (`VERWALTUNG_LAN_CIDRS`), `LEITSTELLE_CIDRS`, `LEITSTELLE_FENSTER_MIN`, `SICHERUNG_FRIST_TAGE` und `HOST_UID` / `HOST_GID` bleiben unverändert. Ist `VERWALTUNG_LAN_CIDRS` leer oder ungültig, fragt er am Terminal danach und schlägt das Netz der eigenen Schnittstelle vor. Ohne Eingabe, ohne Terminal oder mit `--ja` bleibt es beim Hinweis, dass die Anlage im Profil dann nur am Gerät verwaltbar ist. Am Ende weist er auf ein fehlendes Sicherungs-Passwort und auf die Frist der Sicherungen hin. Auf einer Kamera-Erweiterung im Verbund überträgt er nichts, dort gibt die Hauptanlage das Profil vor; er bietet nur an, `VERWALTUNG_LAN_CIDRS` zu setzen, siehe Kapitel Verbund. Vor dem Ändern zeigt er, was sich ändert, und fragt nach. `--ja` übernimmt ohne Rückfrage, ohne Terminal geht es nur so oder mit `PROFIL_OHNE_RUECKFRAGE=1`. Läuft die Anlage schon, stoppt er die laufenden Zusatz-Apps und startet die Anlage mit Neubau neu. Ein zweiter Aufruf ändert nichts weiter. Jede Übernahme steht in `logs/deploy.log`. Einen Befehl zum Abschalten gibt es nicht, abgeschaltet wird mit einer Abschalt-Freigabe, siehe Kapitel Datenschutzprofil.

Wer die Werte von Hand überträgt, setzt `LAN_HTTP=aus` ebenfalls erst nach abgeschlossener Einrichtung und führt danach `./manage.sh restart` aus oder startet in „Anlage verwalten“ neu.

Schlüssel	Wert	Wirkung
`PRIVACY_PROFILE`	`edeka`	Datenschutzprofil an
`PRIVACY_LOCK`	`edeka`	Profilsperre, siehe Kapitel Datenschutzprofil
`PRIVACY_SMTP_HOSTS`	Mailserver des Kunden	Leer heißt: E-Mail gesperrt

Schlüssel	Wert	Wirkung
LAN_HTTP	aus	Im Markt-LAN nur HTTPS, siehe „HTTPS im Marktnetz“
FERNZUGRIFF	aus	Kein Fernzugriff über das Relay, Zugriff über das VPN des Kunden
COMPOSE_PROFILES	knowsora-vision , dazu die Abwahl-Zeilen # suite-removed , # knowsora-localllm-removed , # knowsora-ai-docker-removed	Nur die Bild-KI, Zusatz-Apps abgewählt
VERWALTUNG_LAN_CIDRS	Markt-LAN, z. B. 192.168.10.0/24 , mehrere mit Komma	Admin-Funktionen nur aus diesem Bereich. Leer, ungültig oder ein Bereich über alle Adressen (0.0.0.0/0 , ::/0): im Profil nur am Gerät verwaltbar. Am Gerät (Bildschirm der Anlage) geht die Verwaltung im Profil immer
LEITSTELLE_CIDRS	VPN-Netz der Leitstelle, z. B. 192.168.50.0/24	Prüfzugang /leitstelle/ nur aus diesem Netz. Leer oder ungültig heißt gesperrt. Gilt auch ohne Profil
LEITSTELLE_FENSTER_MIN	60	Minuten ab der Quittung, in denen die Leitstelle einen Alarm ansehen kann, höchstens 240
SICHERUNG_FRIST_TAGE	nicht in der Vorlage, leer heißt 7	Frist der Sicherungen im Profil in Tagen, ganze Zahl von 1 bis 9999
HOST_UID , HOST_GID	Kennung des Betreibers am Gerät	Dienst ohne Rootrechte
GO2RTC_BIND_OPEN	nicht setzen	Stream-Dienst bleibt an die interne Schnittstelle gebunden

Ohne die Abwahl-Zeilen trägt manage.sh update die Standard-Profile der Zusatz-Apps wieder in COMPOSE_PROFILES ein und baut ihre Images. Im Datenschutzprofil stoppt die Anlage die Zusatz-Apps dann nach jedem Start, solange keine Freigabe besteht.

Die Kennzeichenerkennung ist ab Version 2026.11.16 bewusst entfernt, auf jeder Anlage, mit und ohne Datenschutzprofil. LocalEye liest keine Kennzeichen mehr. Das Image enthält weder ihre Bibliotheken noch ihre Modelle, den Schalter ANPR_MODELLE gibt es nicht mehr. Der erste Start nach dem Update löscht die gespeicherte Kennzeichen-Liste, den Verlauf, die Bildausschnitte und die Kennzeichen-Meldungen im Meldungs-Verlauf, im Datenschutzprofil mit Eintrag im Journal. Im Prüfbild, im Vorschaubild, im Clip und in der Leitstellen-Ansicht verpixelt die Anlage bei Fahrzeugen den unteren Teil, wo in der Regel das Kennzeichen sitzt.

> Stand der Prüfung: Version 2026.11.16 läuft auf einer Testanlage ohne Datenschutzprofil. Im Datenschutzprofil, mit echter Leitstelle und im Verbund zweier echter Geräte ist sie noch nicht an einem Gerät mit echten Kameras geprüft. Führen Sie die Abnahme deshalb am Zielgerät durch, bevor der Betrieb beginnt.

Stückliste: Die Release-ZIP enthält die Stückliste aller Komponenten als `SBOM.cdx.json` (CycloneDX 1.5, 486 Komponenten: 454 Bibliotheken, 19 Container, 13 Modelle; 485 mit Lizenzangabe, ohne bleibt nur das Modell `reid_osnet.onnx` für „Person verfolgen“, das nicht ausgeliefert wird) und die Teilliste für den EDEKA-Betrieb als `SBOM-EDEKA.cdx.json` (32 Komponenten, alle mit Lizenzangabe). Beide stehen im signierten Manifest der ZIP. Bibliotheken und Modelle der Kennzeichenerkennung sind nicht mehr enthalten. Ansehen ohne Installation: `unzip -p allinone_whitelabel_release.zip SBOM-EDEKA.cdx.json`.

Abnahme: `sudo ./manage.sh abnahme` im Installationsordner bewertet jede Vorgabe mit OK, ABWEICHUNG oder NICHT PRÜFBAR. Im Container prüft sie die Kennung des laufenden Dienstes, die Root-Marke, die Rechte von `.env` und `users.json`, das wirksame Profil (also auch nur mit `PRIVACY_LOCK`) und ob eine Abschalt-Freigabe die Sperre aufhebt, „Bilder über Token“ und die Schnappschuss-Token-Datei, die aktiven Freigaben mit Name, Begründung und Ende, die Fristen samt längeren Fristen je Kamera, die Voreinstellungen samt Abwahl-Zeilen, `GO2RTC_BIND_OPEN` und `go2rtc_bind_open`, `BIND_HOST`, den Adressbereich der Verwaltung, je Kamera die gespeicherten und die wirksamen Objektklassen, den Voralarm, die Meldekanäle mit erlaubten Mailservern und der Gültigkeit des Prüflinks, den Prüfzugang der Leitstelle (Netz, zweiter Faktor, Kanalbindung, Zeitfenster), die Kennzeichenerkennung (Soll: nicht enthalten, auch keine Modelle aus einem älteren Image), das OSNet-Modell, den Lernlauf und den Clip im Prüflink. Auf einer Erweiterung im Verbund prüft sie die eigene Profilsperre. Am Host kommen die Version im laufenden Image (der Programmcode im Container gegen den Ordner der installierten Version), die laufenden Container, die Rechte von `fernzugriff/frpc.toml`, die Probe über den Tunnel-Eingang der Anlage (Adresse 127.0.0.2: Die Verwaltung muss dort mit 403 antworten und die Leitstellen-Ansicht gesperrt sein, auch wenn der Fernzugriff aus ist), ein Verbindungsversuch zum Relay des Fernzugriffs (Soll: GESPERRT, mit Grund wie Zeitüberschreitung oder Ablehnung; ohne Netz, Route oder Namensauflösung steht dort NICHT PRÜFBAR, weil ohne Adresse keine Sperre belegt ist), die gemessene Bindung von go2rtc und Backend (Soll: nur 127.0.0.1) und im Profil das Sicherungs-Passwort, der tägliche Fristlauf und Sicherungen älter als die Frist dazu. Eine Freigabe ohne Ende oder ohne Begründung zählt als ABWEICHUNG, ebenso eine erteilte Abschalt-Freigabe. Die Zeile „Lernlauf“ ist OK, wenn er aus ist oder eine gültige Freigabe hat, die Zeile „Clip im Prüflink“ nur, wenn der Clip aus ist. Hat das Gerät wegen wenig Arbeitsspeicher auch die Bild-KI abgewählt, zählt das als OK. Der Push-Port steht als NICHT PRÜFBAR da, ob er nur aus dem VPN erreichbar ist, prüft der Errichter am Regelwerk der Firewall. Das Protokoll enthält keine Token, Passwörter, E-Mail-Adressen oder vollständigen IP-Adressen, Begründungen stehen gekürzt darin. Schreiben Sie deshalb keine Zugangsdaten und keine Personennamen in Begründungen und Kameranamen. Das Protokoll geht auf den Bildschirm und nach `logs/abnahme_<Datum-Zeit>.txt` (Rechte 600). Bei Abweichungen endet der Befehl mit Exit-Code 1, läuft der LocalEye-Container nicht, mit 2. Er ändert nichts. Ohne `sudo` kann er den Sicherungsordner nicht lesen, die Zeilen dazu stehen dann als NICHT PRÜFBAR da. Nur den Teil im Container zeigt `docker exec localeye-suite<INSTANCE_SUFFIX> sh /app/edeka_abnahme.sh`. Den vollen Selbsttest zeigt `./manage.sh selbsttest` am Gerät.

5. Erste Einrichtung

Diese Reihenfolge hat sich bewährt.

1. **Zweiter Admin:** Legen Sie sofort ein zweites Admin-Konto an, siehe Kapitel 8.
2. **2FA:** Für weitere Admins bei ihrer ersten Anmeldung einrichten, sie ist Pflicht.
3. **Datenschutzprofil:** Falls gefordert, jetzt einschalten, solange noch keine Daten vorhanden sind.
4. **Kameras:** Per Netzwerk-Scan einbinden.
5. **KI und Zonen:** Je Kamera KI starten, Zonen und Ausschluss-Zonen zeichnen.
6. **Meldungen:** Mindestens einen Kanal einrichten und testen.
7. **Fristen:** Aufbewahrung für Aufnahmen, Snapshots und Meldungs-Verlauf setzen.
8. **Sicherung:** Sicherungsziel wählen, Sicherungs-Passwort setzen und eine erste Sicherung erstellen. Im Datenschutzprofil entsteht ohne Sicherungs-Passwort keine Sicherung.
9. **Probe:** Einmal durchs Bild laufen und prüfen, ob Ereignis, Aufnahme und Meldung ankommen.

> Aufnahmen, Snapshots und KI-Berichte löscht die Anlage ohne eingestellte Frist nicht, der Speicher läuft irgendwann voll. Im Datenschutzprofil gelten höchstens 72 Stunden.

6. Lizenz

Aktivieren: „Anlage verwalten“, Karte Lizenz, oder `./manage.sh activate <Schlüssel>`.

- Die Anlage prüft die Lizenz beim Start, beim Update und alle 24 Stunden.
- Eine einmal bestätigte Volllizenz läuft auch ohne Internet weiter. Eine Störung am Lizenzserver gilt als Netzausfall.
- Eine noch nie bestätigte Anlage hat 48 Stunden Frist. Demos laufen auch offline nach ihrem Datum ab.
- Bei einer ausdrücklichen Ablehnung trennt der Fernzugriff binnen rund 30 Sekunden. Die Bedienung sperrt spätestens mit der nächsten Lizenzprüfung, also bis zu 24 Stunden später. Aufnahme und Erkennung laufen weiter.

> Außerhalb des Datenschutzprofils stoppt eine ausdrückliche Ablehnung bei Start, Neustart und Update alle Dienste, auch „Anlage verwalten“. Dann hilft `./manage.sh activate <Schlüssel>` in der Shell. Beim Aktivieren selbst ändert ein abgelehnter Schlüssel nichts, der bisherige bleibt aktiv. Im Datenschutzprofil laufen Aufnahme und Alarm weiter, einmal gestoppte Dienste startet `manage.sh` aber nicht wieder.

Kamera-Erweiterungen brauchen keinen Schlüssel. Eine ist je Lizenz inklusive, weitere per Erweiterungs-Token unter Einstellungen, Verbund, „Code einlösen“.

7. Datenschutzprofil

Das Profil setzt strenge Vorgaben mit einem Schalter in „Anlage verwalten“, Karte Datenschutzprofil.

Bereich	Wirkung
Aufbewahrung	Höchstens 72 Stunden für Aufnahmen, Snapshots, Berichte und Meldungs-Verlauf. Audit-Journal und Kassendaten haben eigene Regeln, Sicherungen eine eigene Frist (`SICHERUNG_FRIST_TAGE` , leer 7 Tage).
Meldungen	Ohne Bild. Mit Freigabe „Vorschaubild in E-Mail und Push“ geht bei KI-Erkennung und Zonen-Alarm ein Vorschaubild mit, verpixelt wie das Prüfbild: Köpfe der erkannten Personen nach ihrer Lage und Gesichter, bei Auto, Lkw und Bus die unteren 60 Prozent, beim Motorrad das ganze Fahrzeug. Kleidung bleibt erkennbar. Verpixelt werden alle Personen und Fahrzeuge, die die KI im Bild erkennt, auch außerhalb der Zonen und unabhängig von der Objektauswahl der Kamera. Personen zählen dafür schon ab geringer Sicherheit, auch unter der Konfidenz-Schwelle der Kamera, Fahrzeuge ebenso. Ohne gültige Box einer Person oder eines Fahrzeugs geht kein Bild hinaus. Andere Meldungen bleiben ohne Bild, ohne Verpixelung geht nie eines hinaus. Jeder Versand steht im Journal, je Kanal und Kamera höchstens einmal in 10 Minuten. Nur freigegebene Kanäle.
Prüfbild	Kopf nach der Lage der Person: Ist ihre Box niedriger als das 1,6-fache ihrer Breite (gebückt, kniend, liegend), verpixelt die Anlage die obere Hälfte und an beiden Enden einen Streifen über die volle Höhe. Fahrzeuge wie bei den Meldungen. Gilt für Prüflink, Clip, Vorschaubild und Leitstellen-Ansicht.
Token	Kein Kamerabild und kein Video ohne Anmeldung: API-, Schnappschuss- und Leitstand-Token bekommen 410 mit „Im Datenschutzprofil gibt es Kamerabilder nur nach Anmeldung.“, der Weg zum Videodienst mit API-Token 403. Eine Freigabe dafür gibt es nicht. Jede Ablehnung steht gebündelt als „Abruf per Token abgelehnt“ im Journal. Die Schnappschuss-Token-Datei legt die Anlage nicht an und löscht eine vorhandene („Token entfernt“). Scharf/Unscharf und `/metrics` per API-Token bleiben.
Bildbeschreibung	Aus bis zur Freigabe. Ohne Freigabe läuft sie für Prüfhinweis und Griff-Wache nur intern und flüchtig, zum Ereignis wird keine Beschreibung gespeichert oder angezeigt. Mit Freigabe enthält ein Prüfhinweis die Bildbeschreibung als Text.
Kanäle	Aktiv: E-Mail über erlaubte Mailserver, Push-Dienst der Anlage, Leitstelle. Teams und Webhook mit Freigabe, alle anderen gesperrt.
Ton	Keine Tonspur in Aufnahmen, kein Ton im Live-Bild
Funktionen	Aus bis zur Freigabe: Zusatz-Apps, Personensuche, Prüfhinweise, Verhaltens-Erkennung, Griff-Wache, Kassen-Abgleich, Texterkennung (auch die Textsuche in einer Aufnahme, Knopf „Text“), Bildbeschreibung, Vorschaubild in Meldungen, Clip im Prüflink, Lernlauf, iOS-Wecksignal
Gesperrt	Nie freigebbar: Ton in Aufnahme und Live-Bild, Trainings-Export, Ring, Wyze, DoorBird
Kennzeichen	Keine Kennzeichenerkennung: bewusst entfernt, auf jeder Anlage, siehe Kapitel EDEKA-Betrieb

Bereich	Wirkung
Kameras	Jede Kamera zählt Personen und nur Personen, gleich welche Objekte in ihren KI-Einstellungen ausgewählt sind. Die Objekt-Kacheln sind gesperrt, „Person“ steht fest auf an, die gespeicherte Auswahl bleibt und gilt ohne Profil wieder. Soll eine Kamera gar nichts zählen, wird ihre KI ausgeschaltet. Fahrzeuge und Tiere lösen weder Meldung noch Alarm, Bericht, Statistik oder Aufnahme aus, auch nicht über die kameraeigene Erkennung; ihre Position dient nur dem Verpixeln. Kamera-Ereignisse zu Fahrzeug, Tier, Kennzeichen und Parken sowie Smart-Erkennungen ohne Person (Hikvision, ONVIF, Tapo) verwirft die Anlage und zählt sie nur: Der Selbsttest zeigt die Zahl, das Journal je Stunde höchstens einen Eintrag ohne Kamera. Sabotage, Videoverlust und Störungen der Kamera gehen immer durch. Grenze: Die Bewegung, die ein Auto auslöst, meldet eine Hikvision- oder ONVIF-Kamera weiter als „Kamera-Ereignis“. Wer diesen Auslöser am Kanal braucht, schaltet an der Kamera „KI nur bei Kamera-Ereignis“ ein, dann prüft die eigene KI und zählt nur Personen.
Manuelle Aufnahmen	Enden nach höchstens 2 Stunden von selbst
Prüfhinweise	Entscheidungen und daraus gelernte Fehlalarm-Muster werden nach der Regelfrist von 72 Stunden gelöscht. Muster ohne Lerndatum oder mit einem Datum in der Zukunft bekommen im nächsten stündlichen Löschlauf das aktuelle Datum. Importierte Muster tragen im Profil die Importzeit und gelten ab dem Import eine volle Frist.
Lernlauf	Der gespeicherte Bericht des letzten Lernlaufs verliert die Tabelle der einzelnen Rückmeldungen, sobald der Lauf älter als die Frist der Entscheidungen ist (höchstens 72 Stunden). Die übrigen Abschnitte bleiben. Eine Kopie in KnowSora (Freigabe KnowSora-Ablage) fällt nicht unter diese Frist.
Live-Ansicht	Auch das Einzelbild (Kacheln, Vollbild, KI-Bild, Kacheln einer Erweiterung) steht als „Live-Ansicht geöffnet“ mit Nutzer, Kamera und Zeit im Journal, je Nutzer und Kamera höchstens einmal in 10 Minuten. Ebenso der Videodienst für Admins und auf einer Erweiterung Kachel und Video der Hauptanlage (Nutzer `verbund:<Kennung>`). Vorschaubilder von Aufnahmen und der Snapshot-Abruf stehen ebenfalls im Journal. Weitere Aufrufe im Fenster schreibt ein Abschluss-Eintrag als Zahl nach. Ohne Profil schreibt nur das Live-Video diesen Eintrag.
Leitstelle	Zyklische Testmeldung E602 ist Pflicht, ohne eingestellten Takt alle 6 Stunden. Voralarm E138 ist aus und nicht freigebbar.
Verwaltung	Alle Admin-Funktionen samt Einstellungen, Benutzern, Meldekanälen und Scharf/Unscharf (auch per API-Token) nicht über den Fernzugriff, nur aus dem Adressbereich `VERWALTUNG_LAN_CIDRS`. Ohne gültigen Bereich nur am Gerät, auch Scharf/Unscharf per API-Token. Am Gerät (Bildschirm der Anlage) geht die Verwaltung immer, die Anmeldung bleibt nötig. Als „am Gerät“ zählt auch jeder Prozess auf der Anlage, der das Backend ohne die Kopfzeilen des Suite-nginx anspricht, etwa ein weiterer Reverse-Proxy auf demselben Gerät. Abweisungen stehen als „Verwaltung abgewiesen“ im Journal, je Adresse höchstens einmal in der Minute. Im Verbund prüft eine Hauptanlage im Profil den Menschen mit ihrem eigenen Bereich, siehe Kapitel Verbund.
Sicherungen	Nur verschlüsselt mit Sicherungs-Passwort, sonst entsteht keine. Gelöscht nach `SICHERUNG_FRIST_TAGE`. Zurückspielen lässt die `.env` der Anlage stehen. Siehe Kapitel Sicherung und Wiederherstellung.
Stream-Dienst	go2rtc bindet API und RTSP nur an 127.0.0.1. `GO2RTC_BIND_OPEN` und der Schalter `go2rtc_bind_open` wirken nicht, der Selbsttest warnt bei einem gesetzten Schalter.

Bereich	Wirkung
Verifikationslinks	Aus und nicht freigebbar: Im Datenschutzprofil gibt es für die Bildprüfung nur den Prüflink
Fernzugriff	Läuft nur, wenn alle Admins 2FA eingerichtet haben
Trainings-Export	Nicht freigebbar
Lizenz	Eine Ablehnung stoppt keine laufenden Dienste

> Beim Einschalten wird alles Ältere als die Frist endgültig gelöscht. Gehaltene Aufnahmen bleiben. Prüfen Sie vorher, was aufbewahrt werden muss, und setzen Sie Legal Hold.

Mailserver: E-Mail-Meldungen gehen nur über Mailserver, die Sie in der Karte unter „Erlaubte Mailserver“ eintragen und speichern.

Ausnahmen: Freigaben erteilen Sie in LocalEye unter Einstellungen, Funktionen, mit mindestens 20 Zeichen Begründung. Eine Grundlage wie DSFA oder Betriebsvereinbarung ist Pflicht für Person verfolgen, Prüfhinweise und Verhalten, Griff-Wache, Kassen-Abgleich, Clip im Prüflink, Lernlauf, Texterkennung, Bildbeschreibung und die Zusatz-Apps KnowSora, SearchTool und InfraQuill. Das Feld Grundlage zeigt bei der gewählten Funktion an, ob es Pflicht ist. Freigaben, die vor dem Update ohne Grundlage erteilt wurden, bleiben gültig; wer sie verlängert oder neu anlegt, braucht die Grundlage. Die Funktion ist damit sofort an, die Freigabe steht im Protokoll. Die Freigabe Texterkennung schaltet auch die Texterkennung auf Ereignisbildern ein, die sich danach unter Einstellungen, Verbindungen wieder ausschalten lässt.

Befristete Freigaben und Griff-Wache: Clip im Prüflink und Lernlauf gibt es nur befristet. Ohne Enddatum legt die Anlage die Freigabe nicht an; das Enddatum muss ein echtes Datum sein und darf nicht in der Vergangenheit liegen. Ohne gültige Freigabe, also auch nach ihrem Ablauf, sind beide aus, der nächste Profillauf schaltet sie ab. Anders als bei den übrigen Funktionen schaltet die Freigabe beide nicht selbst ein: Den Clip schaltet der Admin danach unter Einstellungen, Verbindungen ein, den Lernlauf unter Leistung. Die Griff-Wache braucht die Freigaben „Griff-Wache“ und „Prüfhinweise und Verhalten“ und läuft erst nach der Bestätigung im Dialog unter Funktionen, Griff-Wache, auf den dort ausgewählten Kameras.

Längere Fristen: Nur für Aufnahmen, Snapshots und Berichte, je Kamera, mit Begründung und Enddatum, höchstens 336 Stunden.

Profilsperre: Mit `PRIVACY_LOCK=edeka` in der `.env` bleibt das Profil in LocalEye aktiv, auch wenn jemand `PRIVACY_PROFILE` leert, und „Anlage verwalten“ verweigert das Abschalten. Erst erteilt ein Admin in LocalEye unter Einstellungen, Funktionen, Karte Datenschutzprofil, mit „Abschalten freigeben“ eine Abschalt-Freigabe mit mindestens 20 Zeichen Begründung, Grundlage optional. Sie steht im Journal, danach lässt sich das Profil in „Anlage verwalten“ abschalten. „Freigabe zurücknehmen“ sperrt wieder, das geht nur, solange das Profil noch an ist. Eine Freigabe gilt für ein Abschalten: Schaltet jemand das Profil danach in „Anlage verwalten“ wieder ein, verfällt sie, und ein erneutes Abschalten braucht eine neue. Solange das Profil abgeschaltet ist, lässt sich keine neue Freigabe erteilen. Die Anlage vermerkt die benutzte Freigabe vor dem Abschalten in `localeye/config/.abschalt_genutzt`; lässt sich der Vermerk nicht schreiben, schaltet sie nicht ab.

Mit gesetzter Profilsperre gilt das Profil auch bei geleertem `PRIVACY_PROFILE` überall gleich: in LocalEye; in „Anlage verwalten“ (die Karte Datenschutzprofil zeigt es als eingeschaltet, das KI-Training ist gesperrt,

der Fernzugriff startet nur, wenn alle Admins den zweiten Faktor haben); in `manage.sh` (kein Update ohne Signatur, keine gestoppten Dienste bei abgelehnter Lizenz, Sicherung nur mit Sicherungs-Passwort und ohne Verläufe, Snapshots und KI-Berichte, Frist der Sicherungen). Erst eine Abschalt-Freigabe mit Begründung in LocalEye hebt das auf. Sind die Einstellungen nicht lesbar, gilt das Profil.

Übersicht: Die Karte Datenschutzprofil unter Einstellungen, Funktionen bietet die „Verarbeitungsübersicht“ mit Fristen und Freigaben zum Herunterladen, etwa für die DSFA. Sie nennt auch die Frist für die Rückmeldungen im Bericht des Lernlaufs.

8. Benutzer, Rechte und Anmeldung

Rollen - **Admin:** Voller Zugriff samt Einstellungen und Verbund. - **Viewer:** Live-Ansicht, Aufnahmen, Snapshots, beschränkbar auf einzelne Kameras. Viewer sehen keine Kamera-Zugangsdaten, im KI-Status nur ihre Kameras, keine Prüfhinweise und auf keinem Weg Bilder der Griff-Wache, auch nicht im Meldungsverlauf oder Export, und von den Einstellungen nur, was ihre Seiten brauchen. - **Leitstelle:** Nur der Prüfzugang der Alarm-Leitstelle unter `/leitstelle/`, ohne Kamera, Zusatz-App und KI, siehe Kapitel Verbund und Leitstelle. Wechselt ein Konto in diese Rolle oder aus ihr heraus, enden seine Sitzungen. Das eigene Konto kann die Rolle weder bekommen noch abgeben. Andere Rollen als Admin, Viewer und Leitstelle nimmt die Anlage nicht an. - **Über den Fernzugriff:** Neue Administratoren lassen sich dort nicht anlegen. Im Datenschutzprofil bewegt niemand Kameras (PTZ) über den Fernzugriff; Kamerabewegungen stehen höchstens einmal je Minute und Kamera im Protokoll.

Benutzer anlegen: Einstellungen, Benutzer, „+ Benutzer“. Änderungen an Rolle und Kameras gelten sofort, eine offene Videoverbindung läuft bis zu ihrem Ende weiter. Ein gelöschter Nutzer verliert den Zugriff sofort.

Feste Kennung: Jedes Konto hat eine feste interne Kennung. Sie bleibt beim Umbenennen erhalten. Wird ein Konto gelöscht und später unter demselben Namen neu angelegt, ist es für die Zusatz-Apps eine neue Person: In KnowSora beginnt es mit einem leeren Konto.

2FA einrichten: Auf den eigenen Namen unten links klicken, Zwei-Faktor-Anmeldung, 2FA einrichten. QR-Code scannen, Code eingeben, die acht Wiederherstellungs-Codes sicher ablegen. Sie werden nur einmal angezeigt. Einrichten können die 2FA in der Oberfläche derzeit nur Admins. Ein Konto der Rolle Leitstelle richtet sie bei seiner ersten Anmeldung unter `/leitstelle/` selbst ein.

2FA-Pflicht: 2FA ist für Admins Pflicht und lässt sich nicht abschalten. Der erste Admin richtet sie in der Einrichtung ein. Jeder weitere Admin kann nach der Anmeldung nichts anderes tun, bis er sie eingerichtet hat.

2FA-Code: Ein Code aus der Authenticator-App gilt nur einmal, auch zwischen LocalEye und „Anlage verwalten“. Wer sich gerade in LocalEye angemeldet hat, nimmt für „Anlage verwalten“ den nächsten Code (höchstens 30 Sekunden warten). Sonst erscheint: „Dieser Code wurde schon verwendet. Bitte den nächsten Code abwarten.“

Sperren: Nach fünf Fehlversuchen wird die Anmeldung von dieser Adresse für 30 Sekunden gesperrt, steigend bis 15 Minuten.

> Halten Sie mindestens zwei Admin-Konten. Passwort und 2FA setzt ein anderer Admin zurück. Für das letzte Admin-Konto bleibt bei der 2FA nur der Befehl am Gerät, für das Passwort gibt es keinen Selbstbedienungsweg.

Verlorenes Handy: Mit einem Wiederherstellungs-Code anmelden. Haben Sie keinen Code und keinen zweiten Admin, hilft am Gerät `./manage.sh 2fa-zuruecksetzen <Benutzer>`, das steht im Protokoll. Ohne Codes setzt ein anderer Admin unter Einstellungen, Benutzer mit dem Knopf „2FA“ zurück, er erscheint nur, wenn der Nutzer 2FA hat. Im Datenschutzprofil geht das für Admin-Konten nur im lokalen Netz.

9. Kameras und NVR

Weg 1, Kameras direkt: Die Anlage bezieht die Streams von den IP-Kameras. Der Netzwerk-Scan findet Kameras per ONVIF, RTSP und Hersteller-Signaturen.

Weg 2, über den NVR: Der NVR zeichnet unverändert weiter auf, die Anlage liest je Kanal den RTSP-Stream. UniFi Protect wird direkt per API-Key angebunden. Protect meldet LocalEye dabei keine Bewegung und keine Smart-Erkennung, mit und ohne Datenschutzprofil. Personen an Protect-Kameras erkennt die eigene KI im Videobild.

UniFi Protect, Zertifikat der Konsole: LocalEye merkt sich beim ersten Kontakt das Zertifikat der Protect-Konsole. Ändert es sich, sendet LocalEye den API-Key nicht mehr dorthin, und der Anlagenwächter meldet eine Störung. Sie geht an die eingerichteten Kanäle, nicht an die Leitstelle. Nach einem Neustart erscheint sie erst wieder beim nächsten Kontakt mit der Konsole. Geben Sie nach einem Tausch oder Zurücksetzen der Konsole den API-Key unter Einstellungen, Verbindungen neu ein; danach gilt das neue Zertifikat.

UniFi Protect, mehrere Konsolen: Weitere Konsolen kommen unter Einstellungen, Verbindungen, „Weitere Protect-Konsolen“ dazu, jede mit Name, Adresse und eigenem API-Key (höchstens acht neben der ersten). Die erste Konsole (Protect Host) bleibt unverändert. Auf der Seite UniFi Protect wählen Sie oben die Konsole und importieren ihre Kameras; eine Kamera merkt sich ihre Konsole und fragt nur diese nach Snapshots und Gegensprechen. Zertifikat, Key und Störung „Zertifikat geändert“ gelten je Konsole, die Störung geht wie bei der ersten nicht an die Leitstelle. Eine neue Adresse verlangt den Key neu. Die Liste der Konsolen steht ohne Keys in settings.json (`protect_weitere`) und geht mit dem Verbund-Backup mit, die Keys liegen nur in der Secrets-Datei. Wird eine Konsole entfernt, bleiben ihre Kameras und zeigen weiter Bild über ihre gespeicherten Stream-Adressen.

UniFi Protect über die UniFi-Cloud: Ist eine weitere Konsole nur über die Cloud erreichbar, wählen Sie die Verbindung „UniFi-Cloud“, fügen den Link der Konsole von unifi.ui.com ein und tragen einen Site-Manager-Schlüssel ein (unifi.ui.com, API, Create API Key, mit dem Konto, dem die Konsole gehört; Konsole ab Firmware 5.0.3). LocalEye spricht dann `https://api.ui.com/v1/connector/consoles/<Konsolen-ID>/…` mit voller Zertifikatsprüfung an. Es kommen nur Schnappschüsse, KI auf diesen Bildern und Zustände; die Kameras werden ohne Videoströme, ohne Aufnahme und ohne Vorlauf angelegt. Ubiquiti begrenzt auf 100 Anfragen je Minute und Konsole: LocalEye nutzt höchstens 80 für Bilder und Zustandsabfrage (Zustand alle 30 Sekunden, Bilder auf die Kameras verteilt, mindestens 2 Sekunden Abstand je Kamera) und hält 15 für die Bedienung frei; antwortet die Cloud mit 429, ruht die Konsole bis Retry-After. Für den vollen Umfang verbinden Sie die Standorte per VPN (Port 443 und 7441 zur Konsole) und stellen die Konsole auf „Lokale Adresse“ mit dem lokalen Key um; ein erneuter Import gibt den Kameras Video und Aufnahme zurück.

UniFi Protect, Weiterleitungen und Secrets: Anfragen an Protect folgen keiner HTTP-Weiterleitung, bei keiner Konsole; der API-Key geht nur an die eingetragene Adresse. Alle Schreiber der Secrets-Datei (API-Token, Leitstand-Token, Verbund-Kopplung, Protect-Keys) ändern sie unter einer gemeinsamen Sperre.

> LocalEye zeichnet Ereignisse auf. Eine Daueraufzeichnung bleibt Aufgabe des NVR.

Praktische Hinweise - Stellen Sie Kameras auf H.264. Der Stream-Dienst wandelt Video nicht um, H.265 läuft nicht in jedem Browser. - Nutzen Sie ein Kamera-Konto, nicht das Cloud-Konto des Herstellers. - Hikvision sperrt die IP-Adresse nach Fehlanmeldungen. Prüfen Sie Zugangsdaten sorgfältig. - Hikvision:

Integrationsprotokoll und ONVIF-Benutzer einrichten. Hik-Connect-Kameras ohne Weboberfläche laufen über ONVIF mit `admin` und dem Bestätigungscode. - Reolink: RTSP und ONVIF in der App einschalten. - Stellen Sie sicher, dass die Uhr der Kamera stimmt.

Erprobt: An echter Hardware sind Tapo, UniFi sowie einzelne Hikvision- und Dahua-Kameras geprüft. Hikvision-NVR und ISAPI sind noch nicht an echter Hardware getestet.

Mitarbeiterbereiche: Pausen-, Sozial-, Umkleide- und Büroflächen werden nicht erfasst. Ins Bild ragende Arbeitsbereiche maskieren Sie an der Kamera.

HTTPS im Marktnetz

Die Anlage bietet neben HTTP einen HTTPS-Port an, Standard 8943, siehe Einstellungen, System. Er reicht intern an denselben Dienst weiter, alle Rechte und Sperren gelten unverändert. Der Fernzugriff bleibt davon unberührt.

- **Zertifikat:** Die Anlage erzeugt beim Start ein selbst signiertes Serverzertifikat für ihre LAN-Adresse (keine Zertifizierungsstelle, 825 Tage). Es verschlüsselt genauso, der Browser warnt aber beim ersten Aufruf. Den Fingerabdruck unter Einstellungen, System mit dem im Browser vergleichen, dann die Ausnahme bestätigen. Ändert sich die LAN-Adresse, entsteht beim nächsten Start ein neues. Ein älteres Zertifikat mit CA-Recht ersetzt die Anlage beim Start selbst.
- **Eigenes Zertifikat:** Unter Einstellungen, System hochladen, nur im lokalen Netz. Die Anlage prüft Kette, Ablauf und Mindeststärke (RSA ab 2048 Bit, EC ab 256 Bit, keine SHA-1-Signatur). Das ist der Weg für Kunden mit eigener Zertifizierungsstelle, die Warnung entfällt dann.
- **Tippfehler:** `http://` auf den HTTPS-Port leitet auf https um.
- **Nur HTTPS:** `LAN_HTTP=lokal` in der `.env`, danach `./manage.sh restart` oder Neustart in „Anlage verwalten“. HTTP antwortet dann nur noch am Gerät selbst und für den Fernzugriff, aus dem Netz gibt es eine Umleitung auf den HTTPS-Port. Der Verbund läuft weiter über HTTP. Greift nur, wenn HTTPS eingerichtet ist, sonst bleibt HTTP offen. Nur für Anlagen auf eigenen Geräten: Integrationen, Proxys oder ein Leitstand mit `http://<anlage>:8987` erreichen die Anlage dann nicht mehr, und HSTS gilt für alle Dienste unter demselben Namen. Ab Werk `an`, also wie bisher.
- **HTTP ohne Inhalte (EDEKA-Betrieb):** `LAN_HTTP=aus`. HTTP liefert aus dem Netz keine Inhalte mehr, auch nicht für die Verbundpfade, nur eine Umleitung auf den HTTPS-Port, und fällt nie auf offenes HTTP zurück. Ist HTTPS noch nicht eingerichtet, schließt die Anlage HTTP-Verbindungen aus dem Netz, die Oberfläche erreicht man dann nur am Gerät selbst. Der Selbsttest prüft beides.

10. KI, Zonen und Prüfhinweise

Modell: Auf der Seite KI-Erkennung ist „Auto“ die empfohlene Wahl, die Anlage wählt das passende Modell für ihre Hardware.

Zonen: Unter „KI/Zonen“ je Kamera. Ist eine Zone gezeichnet, zählen nur Erkennungen, deren Mittelpunkt darin liegt. Ohne Zone zählt das ganze Bild. Ausschluss-Zonen blenden Bereiche aus. Alarm-Zonen lösen Meldungen aus.

Takt: Vorgabe sind 5 Sekunden je Kamera. Die Kopfzeile zeigt verpasste Takte. Unter 2 Prozent ist unkritisch, sonst Intervall vergrößern oder Kameras verteilen. Je Kamera hält ein Abgreifer am Stream-Dienst das neueste Schlüsselbild bereit, bevorzugt aus dem Unterstrom, der Takt wartet so nicht auf einen neuen Verbindungsaufbau. Livebilder und Pre-Roll liegen in einem RAM-Ordner von höchstens 512 MB.

Unbewegte Objekte melden nur einmal und verlängern keine Aufnahme. Eine ruhig stehende Person meldet ebenfalls nicht in jedem Takt neu, erst wenn sie sich deutlich bewegt oder eine Alarmzone betritt.

Prüfhinweise

> Prüfhinweise erzeugen Meldungen über Menschen. Die Funktion ist standardmäßig aus und darf nur mit Betriebsvereinbarung und Datenschutz-Folgenabschätzung betrieben werden.

1. Einstellungen, Funktionen: Prüfhinweis einschalten, im Datenschutzprofil mit Begründung.
2. Kameras mit KI-Erkennung müssen laufen, die Bild-KI ebenfalls.
3. Hinweise erscheinen auf der Seite Prüfhinweise. Die Seite zeigt, wenn die Funktion aus ist oder die Bild-KI nicht antwortet.
4. Jeder Hinweis wird bestätigt (das Beschriebene ist im Bild zu sehen) oder verworfen. Die Seite zeigt daraus den Anteil der Fehlalarme an den bewerteten Hinweisen, mit Zahl der offenen, in Prozent erst ab 20 Bewertungen. Das ist nicht die Fehlalarmquote eines Testprotokolls.

Fehlalarme senken: „5 Minuten kalibrieren“ im KI/Zonen-Dialog, während die Szene normal ist. Verdachtsfälle in diesem Fenster werden zu Normal-Mustern und unterdrücken nahezu gleiche Meldungen. Die Muster sind einsehbar und löschbar. Im Datenschutzprofil gehen „5 Minuten kalibrieren“, Export und Import der Normal-Muster nur mit den Freigaben Prüfhinweise und Bildbeschreibung. Sonst meldet LocalEye: „Im Datenschutzprofil gesperrt: Prüfhinweise und Bildbeschreibung. Freigabe mit Begründung nötig.“

Bildbeschreibung: Ohne Datenschutzprofil an. Im Profil ist sie aus, bis sie in der Karte Datenschutzprofil als Funktion „Bildbeschreibung“ freigegeben wird. Ist sie aus, läuft sie für Prüfhinweis und Griff-Wache nur intern und flüchtig, zum Ereignis wird keine Beschreibung gespeichert oder angezeigt.

Grenzen: Hinweise entstehen aus Einzelbildern und erscheinen mit Verzug. Die Bild-KI beschreibt jedes gespeicherte Ereignis nacheinander, auf der CPU sind das etwa 25 bis 45 Sekunden je Bild. Ohne GPU ist das eine Stichprobe, Zonen-Alarme kommen zuerst.

Verhaltens-Erkennung

Sie meldet langes Verweilen und ist im Datenschutzprofil bis zur Freigabe aus. In Bereichen mit normalem Kundenverkehr, etwa im Supermarkt, entstehen dadurch viele Meldungen. Lassen Sie den Auslöser dort aus.

Speicherordner und Rechte

LocalEye sieht vom Rechner nur die eingestellten Speicherordner, nie ganze Datenträger. Gesperrt sind Systemordner, die Wurzel eines Datenträgers sowie der Installationsordner und alles darüber; darin sind nur `localeye/recordings` und `localeye/snapshots` erlaubt. `/home`, `/opt`, `/var`, `/tmp` und `/snap` gehen nur, wenn ein Ordner dort schon vor dem 03.11.2026 eingehängt war. `manage.sh update` stellt bestehende Anlagen um und legt `docker-compose.yml.vor-speicher` als Sicherung an.

Neuen Speicherordner einrichten: 1. Unter Einstellungen, „Aufbewahrung & Speicherorte“, „Freigegebene Speicherbereiche“ den Ordner auf dem Gerät freigeben, etwa `/volume1/localeye`. Das geht nur im lokalen Netz oder per VPN, nicht über den Fernzugriff und nicht über den Verbund. 2. Unter „Anlage verwalten“ aktualisieren. Das hängt den Bereich ein. 3. Danach den Ordner als Aufnahmen- oder Snapshots-Ordner wählen, etwa `/host/volume1/localeye/aufnahmen`. Die Anlage übernimmt ihn nur, wenn er freigegeben, eingehängt und für den Dienst beschreibbar ist, sonst bleibt der alte.

Ein genutzter Bereich lässt sich nicht entziehen. Würde ein heute genutzter Speicherordner nach einem Update nicht mehr eingehängt, bricht `./manage.sh update` vor der ersten Änderung ab und ändert nichts.

KnowSora sieht LocalEyes Konfiguration nicht, nur einen Auszug ohne Zugangsdaten (`localeye/config/fuer_apps`: Speicherordner, je Kamera Name und Schalter) und die Datenordner lesend. Im selben Auszug zeigt LocalEye in `bildserver_bedarf.json` an, bis wann es den Bildserver für Prüfhinweise oder eine Griff-Prüfung braucht. Der Wert gilt nur wenige Sekunden und wird laufend erneuert; solange er gilt, startet KnowSora keine eigene Bildanalyse.

Startet in KnowSora ein Chat-Lauf oder eine Shell-Sitzung ein Programm, das weiterläuft (zum Beispiel einen Entwicklungsserver), bleibt dessen Temp-Ordner unter `/tmp/ks-sandkasten` im Container des KnowSora-Dienstes bestehen, bis das Programm endet. KnowSora entfernt ihn beim nächsten Lauf, spätestens beim Neustart. Das Protokoll nennt das Programm einmal mit seiner Prozessnummer. Das gilt, wenn die KI-Kommandozeile des Laufs (zum Beispiel Claude Code) von selbst endet. Läuft sie bei Stopp, Zeitlimit, Entzug der Shell-Freigabe oder beim Ablauf einer Shell-Sitzung (60 Minuten ohne verbundenen Browser, spätestens nach 8 Stunden) noch, beendet KnowSora auch diese Programme: Programme außerhalb der Prozessgruppe der Kommandozeile bekommen SIGTERM und zwei Sekunden später SIGKILL, die Gruppe selbst wird wie bisher sofort beendet. Es erkennt sie am Temp-Ordner des Laufs in ihrer Umgebung. Container in der Docker-Sandbox laufen in jedem Fall weiter. Auch der Stopp eines Hintergrund-Auftrags der Projekt-Shell beendet die Programme, die der Auftrag gestartet hat. Ein Hintergrunddienst, den mehrere Läufe teilen (zum Beispiel ein Gradle-Daemon), endet dann mit dem Lauf, der ihn gestartet hat. Beendete Programme eines Laufs holt KnowSora beim nächsten Start eines Chat-Laufs oder einer Shell-Sitzung ab. Bis dahin können im Container des KnowSora-Dienstes Zombie-Einträge stehen; sie belegen nur eine Prozessnummer. Zurückschalten lässt sich das Beenden mit der Zeile `KS_LAUF_ABBRUCH=aus` in `knowsora/data/sandkasten-schalter.env`, danach das KnowSora-Backend neu starten.

Ist bei Claude Code, Codex oder Gemini CLI ein API-Key hinterlegt, bekommt die Kommandozeile nur eine Adresse am Gerät und einen Wegwerf-Schlüssel für diesen einen Lauf; den echten Schlüssel setzt der Schlüssel-Vermittler im KnowSora-Backend erst auf dem Weg zum Hersteller ein. Die Zielbindung legt vor jedem Start Ziel, Proxy und Zertifikate fest: Einstellungsdateien im Projekt- und Login-Ordner einer KI-Kommandozeile lenken keine Anfragen mehr um, und Einstellungen, deren Wert ein Befehl ist, laufen nicht. Eine eigene Adresse, ein Proxy oder ein Zertifikat gehört deshalb in die Umgebung des Dienstes `knowsora-backend` (`docker-compose.yml` bzw. `docker-compose.override.yml`: `HTTPS_PROXY`, `NO_PROXY`, `NODE_EXTRA_CA_CERTS`, für ein eigenes Gateway `ANTHROPIC_BASE_URL` bzw. `GOOGLE_GEMINI_BASE_URL`, eigene Kopfzeilen über `ANTHROPIC_CUSTOM_HEADERS`), ein Zertifikat unter `/etc` im Container. Lässt sich ein Lauf nicht binden, startet er nicht (Gemini CLI ohne seine Einstellungen im Abbild des Backends: Update erneut einspielen). Den Zustand zeigen der Kasten „Version der KI-CLIs“ unter KI-Modelle, AI-Provider und der Selbsttest („Schluessel-Vermittler der KI-Kommandozeilen laeuft“, „Zielbindung der KI-Kommandozeilen aktiv“). Zurückschalten lassen sich beide mit den Zeilen `KS_CLI_VERMITTLER=aus` (die Kommandozeile bekommt wieder den echten Schlüssel) und `KS_CLI_ZIELBINDUNG=aus` in `knowsora/data/sandkasten-schalter.env`, danach das KnowSora-Backend neu starten. Die Shell-Freigabe bleibt Vertrauenssache: Wer sie hat, kann die Abo-Anmeldung im Login-Ordner lesen und dort Dateien ablegen, die in anderen Läufen dieses Eintrags wirken.

Der Dienst startet kurz als root, übergibt die Datenordner an den Nutzer `HOST_UID` und läuft dann ohne Rootrechte und ohne Sonderrechte. Auf einem Speicherordner übernimmt er nur Dateien, die root gehören, nie die anderer Dienste. Gelingt der Wechsel nicht, etwa auf einem Netzlaufwerk, bleibt er root, meldet eine Störung, und der Selbsttest zeigt es. `LOCALEYE_ALS_ROOT=1` in der `.env` erzwingt den alten Weg ohne Störung. Läuft der Dienst als root, ohne dass `LOCALEYE_ALS_ROOT=1` gesetzt ist, legt er die Marke `localeye/config/.laeuft_als_root` an und schreibt eine Warnung ins Log, LocalEye meldet das als Störung. Fehlt `HOST_UID` in der `.env`, nimmt Compose die Kennung 1000.

`manage.sh` schließt bei `start`, `restart`, `update` und `restore` Konfiguration, Relay-Zugang und `.env` für fremde Konten des Geräts und nimmt ihnen Schreibrechte in der Installation.

Fehlt der Datenträger eines Speicherordners, zeichnet die Anlage nicht auf und meldet eine Störung, statt unbemerkt auf die Systemplatte zu schreiben. Das erkennt sie an der Datei `.localeye-speicher` im Ordner. Nach einem Plattentausch unter Einstellungen, System auf „Datenträger getauscht“ klicken. Normales Speichern hebt den Schutz nicht auf.

Fristen: Anlagen, die nie eine Löschfrist hatten, bekommen 14 Tage Vorlauf. Die Anlage kündigt das als Hinweis in der Seitenleiste und über alle aktiven Meldekanäle außer der Leitstelle an, zwei Tage vor Ablauf noch einmal. Danach gelten für Aufnahmen und Bilder 3 Tage, für Berichte 3 Jahre. Ein geleertes Fristfeld führt zurück zum Standard, 0 heißt unbegrenzt und verlangt eine Bestätigung, die im Journal steht.

Berichte kürzen: Sobald ein Bild gelöscht ist, verliert auch sein Bericht Vorschaubild, Beschreibung und Text der Bild-KI, es bleiben Zeit, Kamera, Zone und Erkennung. Das erste Kürzen kündigt die Anlage 14 Tage vorher als Hinweis an. Bilder, Berichte und Indexzeilen zu Aufnahmen unter Legal Hold bleiben vollständig, auch von Hand ausgelöste Snapshots derselben Kamera aus dem Zeitraum der Aufnahme, mit zwei Minuten Rand.

Updates brauchen eine gültige Signatur, eine Einstellung zum Abschalten gibt es nicht mehr. Nur für eigene Builds am Gerät: `./manage.sh update --ohne-signatur <zip>` am Terminal, mit Eingabe von `UNSIGNIERT` und Eintrag im Deploy-Log, im Datenschutzprofil nie.

Griff-Wache

> Die Griff-Wache erzeugt Hinweise über Menschen. Nur mit Betriebsvereinbarung und Datenschutz-Folgenabschätzung betreiben.

Die Griff-Wache ist das wichtigste Merkmal von LocalEye zur Diebstahlerkennung und Teil des Release. Ihr Ergebnis ist ein Prüfhinweis, über den ein Mensch entscheidet, keine Feststellung und kein Echtzeit-Alarm. Ob sie einen Griff erkennt, hängt vom Kamerawinkel ab. Wie oft sie im Ladenbetrieb richtig oder falsch anschlägt, ist noch nicht gemessen. Stand: Sie ist im Release und auf der eigenen Testanlage des Herstellers in Betrieb. Mit Version 2026.11.18-1522 ergaben fünf nachgestellte Diebstähle an echten Kameras, abgespielt in vier Taktlagen, in allen 20 Läufen einen Hinweis und 32 Alltagsaufnahmen in 128 Läufen keinen; live an der Kamera ist ein Hinweis dieser Version noch nicht nachgestellt, die Abnahme im Markt steht aus.

Ab Werk ist sie aus, auch für neue Kameras, und ein Update schaltet sie nie ein. Eingeschaltet wird sie unter Einstellungen, Funktionen, Griff-Wache, mit Bestätigung im Dialog und Auswahl der Kameras. Sie braucht zusätzlich die Prüfhinweise und läuft nur an Kameras mit laufender KI-Erkennung. Im Datenschutzprofil braucht sie zusätzlich die Freigaben „Griff-Wache“ und „Prüfhinweise und Verhalten“, jeweils mit Begründung und Grundlage.

Was sie meldet: nur mögliches Einstecken, nicht das Anfassen von Ware.

1. Die Anlage wertet den Unterstream jeder ausgewählten Kamera dauerhaft mit 3 Bildern pro Sekunde aus, auch im leeren Raum. Ein Griff dauert Sekunden, eine Wache, die erst mit der ersten erkannten Person anläuft, käme zu spät. Bewegt sich etwas, sucht die Wache sofort nach Personen, danach kommen sie aus dem KI-Takt. Das Skelett läuft nur, wenn sich bei der Person etwas bewegt.
2. **Einstecken:** Die Hand geht an eine Einsteckstelle, an Hüfthöhe (Hosentasche, Bund, Handtasche an der Seite) oder sie verschwindet direkt aus der Haltung vor dem Körper, etwa unter die Jacke. Wo die Ware genommen wurde, spielt keine Rolle (seit 18.11.2026; bis dahin nur nach einem Griff ins Regal kurz davor): Wer sie an einer Stelle aus dem Regal nimmt und an einer anderen einsteckt, wird ebenso geprüft. Ohne Griff ins Regal kurz davor zählt nur benannte Ware wie beim Gedächtnis (ein Name aus der Warenliste, etwa Flasche, Buch, Schachtel; nicht Karte, Zettel, „small black object“), auch für den Hinweis „Verbleib nicht zu sehen“, und der Hinweistext nennt dann keinen Griff ins Regal. Ware vor Bauch oder Brust halten und ansehen zählt nicht. Im Sitzen prüft die Wache nie; wer in der Hocke ans untere Regal greift, gilt bisher ebenfalls als sitzend.
3. **Bild-KI:** Sie sieht nur den Ausschnitt um die Hand. Sie beschreibt ihn und nennt in einer zweiten, kurzen Frage, was die Hand hält, oder „nichts“; „nichts“ gilt vor einem Gegenstand, den die Beschreibung erfindet, aber nur, wenn die Beschreibung eine Hand zeigt, die Ware vorher benannt war (Name oder Gedächtnis; „medical device“ oder „stick“ reichen nicht), die Beschreibung kein klar gehaltenes, unbenanntes Ding sieht („a blue object“) und nicht dieselbe Ware wie vorher nennt. Gefragt wird nur, wo die Antwort entscheidet. In der anderen Hand gewinnt klare Ware der Beschreibung immer. Sie muss vorher Ware in der Hand sehen und danach, 2 und 5 Sekunden später, keine Ware mehr in der sichtbaren Hand, oder das Einstecken ausdrücklich beschreiben. Ist die Hand danach nur verdeckt, etwa weil sich jemand mit der Ware wegdreht, gibt es keinen Hinweis, außer die Bild-KI hat das Einstecken selbst beschrieben. Unsichere Aussagen („scheint leer“) zählen nicht. Eigene Sachen (Handy, Zigarette, Geld) zählen nie als Ware: wenn der Blick 2 Sekunden vor der Bewegung sie zeigt, oder wenn nur das Bild an der Tasche sie nennt und der frühe Blick keine klare Ware zeigt (an der Tasche ist die Hand oft halb verdeckt, die Bild-KI rät dort kleine Gegenstände).

4. **Person geht:** Ist die Person zum Blick nach 2 und 5 Sekunden nicht mehr im Bild, lautet der Hinweis „Ware genommen, Verbleib nicht zu sehen“, wenn der Blick 2 Sekunden davor benannte Ware zeigte, die das Bild an der Tasche nicht mehr klar in der Hand zeigt, oder wenn bestätigte Ware zuletzt in dieser Hand lag (Gedächtnis). Zeigt auch das Bild an der Tasche die Ware noch klar, trägt die Person sie offen: kein Hinweis (Gegenprobe: Wasserflasche aus dem Raum getragen). Unbenannte Dinge („device“, „small object“) reichen nie. Ob die Person noch da ist, prüft die Wache zum Blick mit einem frischen Skelett, nicht mit dem Rahmen der letzten Personensuche (der steht bis zum nächsten KI-Takt still). Der Hinweis entsteht nur, wenn die Person seit der Bewegung allein im Bild war, und zählt zur selben Obergrenze wie an Kameras mit dem Schalter „Ablage nicht sichtbar“: höchstens sechs je Kamera und Stunde, je Person einer in der Minute.
5. **Hinweis:** Erst dann entsteht ein Prüfhinweis mit vier Bildern: -1 s, Griff mit Rahmen um die Hand, +2 s, +5 s. Er lautet „möglicherweise eingesteckt, ungesichert“ und nennt den Grund: Hand danach ohne Gegenstand, Einstecken beschrieben oder zuvor getragene Ware nicht mehr zu sehen; im Fall 4 „Ware genommen, Verbleib nicht zu sehen“. Ohne eingeschaltete Bildbeschreibung, im Datenschutzprofil also ohne deren Freigabe, ist es je Fall ein fester Satz ohne den Namen des Gegenstands. Ob eingesteckt wurde, entscheidet der Mensch, der Hinweis behauptet keinen Diebstahl.

Mehrere Bewegungen: Nach einem geprüften Griff wartet die Wache bei dieser Person 8 Sekunden, damit dieselbe Bewegung nicht doppelt zählt. Eine neue Bewegung einer Hand (die Hand war erst nach dem letzten geprüften Griff dieser Hand wieder draußen) prüft sie trotzdem, höchstens drei Griffe je Person in 30 Sekunden. Ein Vorfall, ein Hinweis: Ergab schon ein Griff derselben Person in den letzten 30 Sekunden einen Hinweis, bleibt der Griff aus der Pause ohne eigenen (Bild-KI und Gedächtnis laufen trotzdem). Grifftest vom 18.11.2026: Die Hand ging zuerst ans Gesicht, das galt als Griff; die Pause danach verschluckte das echte Einstecken 4 Sekunden später.

Getragene Ware: Bestätigt die Bild-KI bei einem geprüften Griff benannte Ware, die danach noch in der Hand ist, merkt sich die Wache das je Kamera und Person bis zu 60 Sekunden: den Namen, den die Bild-KI nennt, die Hand und die Zeit, nur im Arbeitsspeicher. Solange gilt die Person als „trägt Ware“. Geht bei einem weiteren Griff die Hand unter die Kleidung und ist die Ware danach in keiner Hand mehr klar zu sehen, entsteht der Hinweis auch, wenn die Bild-KI die Ware beim Griff selbst nicht sieht. Dasselbe gilt, wenn die Ware zuletzt in der Hand dieses Griffs lag und die Person danach das Bild verlässt (auch wenn ein Blick sie noch am Bildrand zeigte). (Den Folgegriff mit eigener Obergrenze gibt es seit 18.11.2026 nicht mehr: Jeder Griff wird voll geprüft.) Als „unter Kleidung“ zählt: Die Hand verschwand von vorn gesehen und lag zuletzt an der Körpermitte, der Weg an den Bund endet an der Körpermitte, oder die Hand läuft an der Körpermitte vom Kragen abwärts. Ware vor dem Bauch ansehen, den Reißverschluss hochziehen, die Hosentasche vorn und die Jackentasche an der Seite zählen dafür nicht. Vergessen wird nach einem Hinweis, bei Korb und Wagen, nach einem Griff in eine eingezeichnete Regalzone und in einer Griff-Ausnahme. Für Hinweise gilt das Gedächtnis nur, solange die Person allein im Bild ist. Eigene Sachen (Handy, Geld, Brille, Kassenbon, Tasche) und vage beschriebene Gegenstände werden nie gemerkt.

Keinen Hinweis ergeben Einkaufswagen und Einkaufskorb, leere Hände, Kleidung, Kind, Hund, Kinderwagen und Kassenbon. Greift dieselbe Hand nach dem Griff an die Tasche gleich wieder ins Regal, gilt die Ware als zurückgestellt. Eigene Sachen wie Handy, Zigarette oder Tasse zählen nie als Ware.

Wer den Hinweis sieht: nur Admins, auf der Seite Prüfhinweise. An Meldekanäle geht er nur, wenn dort der Auslöser „Griff-Hinweis“ ausdrücklich gewählt ist, ab Werk ist er das nicht. Er geht nie an die Leitstelle, kommt ohne Verifikationslink und höchstens einmal je Kamera und Kanal in 10 Minuten. In der Liste bleibt jeder Hinweis.

Bewerten: „Bestätigt“ heißt, das Einstecken ist im Verlauf zu sehen, beim Hinweis „Ablage nicht sichtbar“ die Ware in der Hand und danach die Hand ohne sie, beim Hinweis „Verbleib nicht zu sehen“ die Ware in der Hand, bevor Hand und Person aus dem Bild verschwinden. „Fehlalarm“ löscht Verlaufsbild, Ereignisbild, Vorschau und Beschreibung sofort, auch im Meldungsverlauf und in der Kopie der Hauptanlage im Verbund. Es bleibt nur die Entscheidung, und kein Kanal bekommt den Hinweis danach noch. Eine Meldung, die schon unterwegs war, lässt sich nicht zurückholen, die Oberfläche sagt das dann dazu. Unter Legal Hold bleibt alles gesperrt und wird nach der Aufhebung gelöscht. Klappt ein Schritt nicht, sagt die Oberfläche das, und der nächste Aufräumlauf holt ihn nach. Bewertungen und ihr Aufheben stehen ohne Notiztext im Journal.

Daten: Skelette und Bilder bleiben ohne Treffer nur kurz im Arbeitsspeicher. Das Gedächtnis für getragene Ware liegt nur im Arbeitsspeicher und gilt höchstens 60 Sekunden. Mit Treffer gilt für den Hinweis die normale Aufbewahrung. Griff-Hinweise gehen nicht in Trainingsdaten oder Exporte, und Bewertungen daraus erzeugen keine Normal-Muster.

Kameras und Ausnahmen: Kameras kommen nur über den Dialog unter Funktionen dazu. Abschalten geht je Kamera unter KI-Erkennung, Konfigurieren, „Griff-Wache und Verhaltens-Erkennung“. Kasse und Bereiche des Personals nimmt die Zonenart „Griff-Ausnahme“ im Zonen-Editor aus, dort beobachtet die Wache niemanden. Regale zeichnen Sie optional mit der Zonenart „Regal“ ein: Ohne Regalzonen zählt jedes Greifen neben dem Körper im Stehen als Griff ins Regal, mit Regalzonen nur ein Griff, bei dem die Hand in einer Regalzone liegt. Das senkt Fehlhinweise, etwa an der Kasse oder am Ausgang.

Verdeckter Unterkörper, Ablage nicht sichtbar: Am zuverlässigsten arbeitet die Wache, wenn die Kamera die Person bis zur Hüfte zeigt. Mit geschätzter Hüfte rechnet die Wache nur für Personen, deren Unterkörper nachweislich verdeckt ist: Der Rahmen aus der Personensuche endet über der Hüftlinie (Schulter plus Rumpf aus Schulterbreite und längerem Oberarm, je Person der Median der letzten Schätzungen). Reicht der Rahmen tiefer oder passt kein Rahmen zur Person, rechnet sie in jedem Bild wie bisher mit dem gelieferten Skelett, auch ohne Maß, wenn die Hüfte fehlt: An Kameras mit voller Sicht ändert sich nichts, gleich wie sicher MoveNet die Hüfte meldet oder ob jemand sie kurz verdeckt. Der Rahmen kommt in der Anlage aus dem Takt der Kamera-KI (ab Werk alle fünf Sekunden) und ist bei der Übergabe schon alt; die Wache misst ihn am Skelett aus seinem Bild. Seine Unterkante gilt als Kante des Vordergrunds nur, solange die Person seitdem am Platz blieb (Schultermitte höchstens eine halbe Rumpfhöhe daneben, Größe im Band 0,8 bis 1,25). Sonst kennt die Wache bis zum nächsten Rahmen keine Kante. Bei verdecktem Unterkörper zählt eine gemeldete Hüfte nur, wenn beide Seiten sicher zu sehen sind oder eine Seite sicher ist und der Rumpf zur Schätzung passt, wenn die Kante bekannt ist und die Hüfte nicht darunter liegt, und erst im zweiten Skelett in Folge; sonst entscheidet der nächste passende Rahmen, ob die Hüfte wieder zu sehen ist. Mit geschätzter Hüfte zählt nur, was verschwindet, und zwar erst im zweiten Bild in Folge; liegen zwei Handgelenke an derselben Stelle, zählt das sicherere. Taucht die Hand während eines laufenden Verschwindens kürzer als drei Bilder in Folge wieder auf (hinter dem Vordergrund rät MoveNet das Handgelenk immer wieder kurz an die Kante), bleibt sie für die Wache verschwunden. Verschwindet die Hand auf der Brust (höchstens eine halbe Rumpfhöhe unter der Schulter, nah an der Körpermitte, dort sicher gemeldet oder in zwei Skeletten in Folge gesehen) und mindestens 0,3 Rumpfhöhen über der Kante, läuft der Griff wie sonst; ebenso, wenn sie an der Körpermitte vom Kragen abwärts lief und so weit über der Kante endete. Taucht sie danach zuerst näher als 0,3 Rumpfhöhen an der Kante wieder auf, wird der Griff umgestuft. Alles andere ist ein Griff „ohne Sicht“, auch jedes Verschwinden ohne bekannte Kante: Die Wache meldet ihn nur, wenn an der Kamera unter KI-Erkennung, Konfigurieren „Ablage nicht sichtbar“ eingeschaltet ist. Ab Werk ist der Schalter aus, er lässt sich nur an Kameras der Griff-Wache setzen, das Journal hält jedes Ein- und Ausschalten fest, er geht mit aus, wenn die Kamera die Griff-Wache verlässt (wird sie unter Funktionen, Griff-Wache

abgewählt, steht im Journal die neue Kameraauswahl, kein eigener Eintrag zum Schalter), und an allen Kameras, wenn die Funktion Griff-Wache ausgeschaltet wird. Hält das Datenschutzprofil die Griff-Wache nur an (Freigabe abgelaufen oder entzogen), bleibt der Schalter gespeichert und gilt wieder, sobald die Wache an der Kamera weiterläuft. Nur Admins sehen ihn in der KI-Konfiguration. Ohne Schalter fragt die Wache die Bild-KI nicht, setzt keine Pause und vergisst die gemerkte Ware der Person; ein umgestufter Griff gibt Pause und Platz sofort wieder frei. Mit Schalter nimmt jeder der beiden Blicke das erste Bild, in dem MoveNet die Hand sicher meldet und der Handausschnitt im Bild liegt (der erste ab einer Sekunde nach dem Griff, der zweite bis acht Sekunden danach; wartet der Griff auf den Abgang, bis 30 Sekunden, siehe unten). Das gilt auch unter der Kantenlinie, denn ein Vordergrund reicht selten über die ganze Bildbreite; für das Verschwinden selbst zählt eine Hand unter der Kantenlinie weiter als verdeckt. Kommt bis zum Ende der Frist kein solches Bild, zählt das beste, in dem die Hand deutlich über der Kante lag oder nur am Bildrand zu sehen war. Es zählt der letzte Blick auf die Hand, ein nur vorher beschriebenes Einstecken reicht nicht, und Einrichtung wie Türgriff, Stuhl oder Tisch gilt weder vorher als Ware noch danach als „hält die Ware noch“. Für den Satz der Bild-KI zum Blick genügt, dass er die Person beschreibt und keine klare Ware nennt, auch mit einem unsicheren Zusatz dahinter; ohne Aussage bleibt er, wenn unklar ist, ob etwas in der Hand liegt („may be holding“), oder wenn die Hand laut Satz außerhalb des Bildes ist. War die Person länger als eine Sekunde nicht zu erkennen, nimmt der Blick nur ein Skelett an derselben Stelle in derselben Größe; nach einem leeren Bild keines mehr. Der Hinweis lautet „Ware genommen, Hand leer zurück, Ablage nicht sichtbar“, ohne ausdrücklich leere Hand „Ware genommen, danach nicht mehr klar in der Hand, Ablage nicht sichtbar“. Beschreibt die Bild-KI an der wieder sichtbaren Hand ein Einstecken, lautet er wie sonst „möglicherweise eingesteckt, ungesichert“ und sagt, dass die Hand aus dem Blick der Kamera verschwand. Ohne Hüfte im Bild merkt die Anlage als getragene Ware nur, was nach dem Verschwinden wieder in einer Hand zu sehen war. Gemerkte Ware allein genügt für einen Griff ohne Sicht nicht: Die Ware muss bei diesem Griff in der Hand zu sehen sein, und ohne laufenden Folgegriff muss dieselbe Hand binnen 15 Sekunden nach dem Griff ins Regal verschwinden. Sitzen: Wer bei freier Sicht auf den Unterkörper mit Hüfte und Knien sitzend zu sehen war, gilt 20 Sekunden weiter als sitzend, wenn danach etwas die Hüfte verdeckt; wer von Anfang an hinter einem Tisch sitzt, gilt nicht als sitzend. An Kassen, Theken mit Personal und Sitzplätzen gehört deshalb eine Griff-Ausnahme, sonst kommen dort Hinweise. Nachspiel einer Aufnahme wie im Betrieb: `tools/probe/griff_nachspiel.py` mit `--takt 5` (Rahmen im Takt der Kamera-KI; mit `--takt 5:2:1.7` zwei Sekunden Verzug und erster Takt bei Sekunde 1,7, mehrere Versätze durchspielen), `--ohne-sicht` für den Schalter.

Eigener Auslöser an Kameras mit „Ablage nicht sichtbar“: Der Absatz oben beschreibt die bisherige Erkennung. Sie hängt am Rahmen der Personensuche: Rahmt die Suche einen Vordergrund mit ein (Rucksack, Stuhllehne), reicht der Rahmen unter die Hüfte, die Wache schätzt nicht und hat ohne Hüfte kein Maß; zwischen zwei Suchen folgt der Rahmen außerdem den sicher erkannten Punkten und kann bis auf den Kopf schrumpfen. So blieb am 17.11.2026 ein nachgestellter Diebstahl an einer tief stehenden Kamera still. An Kameras mit dem Schalter läuft deshalb seit `2026.11.17-1316` zusätzlich ein eigener Auslöser, solange genau eine Person bekannt ist. Die bisherige Erkennung bleibt daneben unverändert, auch ihr Skelett-Modell; meldet sie dasselbe Verschwinden derselben Hand schon als Griff ohne Sicht, kommt es kein zweites Mal, und neben einem Griff mit Sicht von ihr läuft der neue nur für den Abgang mit. Er ändert ihre Entscheidungen nicht: eigene Plätze im Nachlauf (vier) und in der Warteschlange der Bild-KI (zwei je Kamera), kein Verbrauch ihrer Vorrangplätze bei der Bild-KI, keine Folgegriffe für sie, und das Gedächtnis für getragene Ware liest und schreibt er nicht. Hat er einen Fehler (etwa im größeren Skelett-Modell), setzt er eine Minute aus; die bisherige Erkennung läuft weiter, unter „Zuletzt“ steht es, und nach drei Fehlern in fünf Minuten meldet der Wächter die Störung `griff_oben:<Kamera>`. Der eigene Auslöser rechnet auf einem eigenen Rahmen: dem Rahmen der Personensuche, nach unten verlängert,

bis er anderthalbmal so hoch wie breit ist (höchstens bis zum Bildrand); zwischen zwei Suchen wandert er mit der Schultermitte und behält seine Größe. Darauf rechnet das größere Skelett-Modell (MoveNet Thunder), wenn die Datei im Image liegt, sonst das schnelle. Der Rumpf ist immer aus Schultern und Oberarmen geschätzt. Die Regeln: Ein Griff ins Regal ist eine Hand in Greiflage (neben dem Körper in Greifhöhe, mit Regalzonen in einer Zone); er gilt 15 Sekunden für die Person, nicht für eine Hand. Ein Beleg ist eine Hand, die das Modell sicher meldet (ab 0,5) und die nicht in Greiflage liegt, und zwar nach einem Griff ins Regal (höchstens 15 Sekunden danach); beim Verschwinden zählt er höchstens 15 Sekunden. Eine sicher gemeldete Hand in Greiflage steckt im Regal, sie ist kein Beleg, und was sie davor hielt, gilt als zurückgestellt; ebenso nach zwei Skeletten in Folge, in denen das Modell die Hand nur schwach (ab 0,25) in Greiflage meldet; das gilt auch für einen Griff, der nach dem Verschwinden noch wartet. Liegen zwei Handgelenke an derselben Stelle, zählt das sicherere. Verschwunden ist die Hand, wenn sie anderthalb Sekunden nach dem letzten Beleg nicht sicher zu sehen ist und zuletzt zwei Skelette in Folge verdeckt war. Dann reiht die Wache einen Griff ohne Sicht ein, mit dem sichersten Belegbild der letzten anderthalb Sekunden und ohne frühen Blick. Sitzen und die Regel „erst die Tasche verlassen, dann ins Regal greifen“ kennt dieser Auslöser nicht (ohne Beine und Hüfte im Bild nicht messbar); eigene Sachen schützt dort die Bild-KI und die Frist nach dem Griff ins Regal. Nach einer Lücke von mehr als einer Sekunde gelten Belege und Griff ins Regal nur weiter, wenn die Person an derselben Stelle in derselben Größe wieder da ist; verglichen wird das Maß des neuen Skeletts (ohne sichtbaren Ellbogen nur der Ort).

Abgang: Hat nach einem Griff ohne Sicht noch kein Blick die Hand gezeigt, wartet der Griff an einer Kamera mit dem Schalter bis zu 30 Sekunden auf die Hand (bisher acht). Kommt sie sicher ins Bild, entscheidet der Blick wie bisher. Findet die Personensuche vorher zweimal in Folge niemanden, meldet die Wache den Griff als Abgang, gleich ob er aus dem eigenen Auslöser oder aus der bisherigen Erkennung stammt. Voraussetzungen: frischer Griff ins Regal, kein Folgegriff, die Person war seit dem Griff allein im Bild, dieselbe Hand griff nicht wieder sicher ins Regal, und es ist der jüngste Griff ohne Sicht dieser Hand (ein neuer derselben Hand löst den wartenden ab, gleich aus welchem Auslöser). Kein Abgang, wenn die Person in eine Griff-Ausnahme getreten ist (die Personensuche findet dort mehr Personen als in der Suche der letzten 30 Sekunden, in der dort am wenigsten standen), wenn der Griff nur neben einem Griff mit Sicht der bisherigen Erkennung mitläuft und deren Blick die Hand wieder zeigte, wenn das größere Skelett-Modell die Hand eines Griffs der bisherigen Erkennung nach dem Verschwinden wieder sicher sah, oder wenn der eigene Auslöser wegen eines Fehlers aussetzt. Ein Folgegriff löst keinen wartenden Griff ab. Die Anlage fragt die Bild-KI dann einmal, zum Belegbild: Ein Hinweis entsteht nur, wenn der Satz klar gehaltene oder getragene Ware nennt (mit einem Verb des Haltens oder Tragens; ein Satz, der nur ein Ablegen beschreibt, genügt nicht; kein vager kleiner Gegenstand, keine Einrichtung, kein eigenes Teil) und weder Korb noch Wagen. Der Text lautet „Ware genommen, Verbleib nicht zu sehen, ungesichert“ und sagt, dass die Person den Gegenstand auch offen in der Hand, im Wagen oder im Korb tragen kann. Je Kamera entstehen höchstens sechs solche Hinweise je Stunde und zu einer Person einer in 60 Sekunden; darüber fragt die Anlage die Bild-KI nicht. Bleibt die Person 30 Sekunden im Bild, ohne dass die Hand wiederkommt, endet der Griff ohne Hinweis.

Skelett und Rahmen „Gegenstand“: Der Knopf mit dem Strichmännchen neben dem Live-Knopf blendet das Skelett im Live-Bild ein, die Hand in der Griff-Zone wird gelb. Das dient dem Einrichten und läuft dem Video etwas hinterher. Gilt eine Person als „trägt Ware“, sehen Admins um diese Hand zusätzlich den Rahmen „Gegenstand“, ohne Namen des Gegenstands, bis zu 60 Sekunden lang. Er erscheint nur, wenn die Bild-KI zuvor bei einem geprüften Griff an Tasche, Bund oder Kleidung Ware bestätigt hat, die danach noch in der Hand war. Nach dem Griff ins Regal allein und beim einfachen Ablauf mit nur einem Einstecken erscheint er nicht. Viewer sehen weder den Rahmen noch die gelbe

Hand, die Rolle Leitstelle erreicht das Skelett gar nicht. Skelett und Rahmen sind Punkte und ein Rechteck, kein Bild. Ein Admin bekommt sie auch über den Fernzugriff und über den Verbund, ohne eigenen Eintrag im Journal.

Prüfen: Die Kachel Griff-Wache auf der Seite KI-Erkennung zeigt geprüfte und bestätigte Griffe des Tages, Griffe, die die Bild-KI nicht mehr geschafft hat, je beobachteter Kamera die Bilder pro Sekunde und je Kamera die Griffe ohne Sicht auf die Ablage, die sie heute nicht geprüft hat, weil der Schalter dort aus ist (im Log „Griff ohne Sicht auf die Ablage“). Die Seite Prüfhinweise zeigt für den Zeitraum Hinweise, Bestätigungen und Fehlalarme der Griff-Wache. Störungen meldet der Wächter, wenn die Wache eingeschaltet ist, aber keine Kamera beobachtet, wenn eine Kamera fünf Minuten unter 2 Bildern pro Sekunde liegt oder wenn sie wiederholt Fehler meldet. Wird der Rechner knapp (CPU über 92 %), starten keine leeren Wachen mehr, ab 97 % weichen sie nach und nach. Das Log schreibt `[Griff]`-Zeilen, darunter die Antwort der Bild-KI (im Datenschutzprofil nur deren Länge) und den Grund, warum ein Griff ohne Hinweis blieb. „Kein Platz“ heißt, dass bereits die Höchstzahl an Wachen läuft (60, ab 7 Kernen zehnmal die Kernzahl). Dann kommt jede Kamera nach 60 Sekunden reihum dran. Unter „Zuletzt“ zeigen die Kachel (jüngster Eintrag aller Kameras) und der KI-Dialog jeder Kamera (die letzten drei), was die Wache dort entschieden hat und warum, mit Uhrzeit: Hinweis erstellt, kein Hinweis, weil die Bild-KI vorher keine klare Ware nannte, weil Korb, Wagen oder Regal im Spiel war oder weil die Ware danach noch in der Hand war, nicht geprüft ohne Griff ins Regal davor, ohne Antwort der Bild-KI, wegen der Obergrenze des Abgangs, weil zu dieser Person eben schon ein Hinweis entstand (melden der eigene Auslöser und die bisherige Erkennung denselben Vorfall, entfällt der zweite, wenn die beiden Griffe höchstens 30 Sekunden auseinanderliegen; einen Griff der bisherigen Erkennung prüft die Bild-KI dabei wie immer, nur sein Hinweis entfällt; zwei Griffe der bisherigen Erkennung allein bleiben zwei Hinweise) oder weil der Schalter „Ablage nicht sichtbar“ aus ist; ebenso, wenn die zusätzliche Erkennung für „Ablage nicht sichtbar“ einen Fehler hatte und eine Minute aussetzt (die übrige Griff-Wache läuft weiter). An Kameras ohne den Schalter steht dort auch, wenn der Wache bei einer Person neun Skelette in Folge (drei Sekunden) das Körpermaß fehlte, einmal je Person; das kommt auch an Kameras mit voller Sicht vor, wenn jemand am Bildrand steht. Die Einträge sind feste Texte ohne Satz der Bild-KI und ohne Angabe zur Person, liegen nur im Arbeitsspeicher (je Kamera die letzten fünf, derselbe Grund hintereinander als ein Eintrag mit der jüngsten Uhrzeit; angezeigt werden die der letzten 24 Stunden, Einträge eines anderen Tages mit Datum) und sind nur für Admins sichtbar.

Last: Ein gemeinsamer Lese-Faden und ein Rechenpool mit fester Größe bedienen alle Kameras. Bei Andrang sinkt je Kamera die Bildrate, die Last bleibt gleich. Gemessen am 02.11.2026 auf dem Pentium Gold 8505 mit Unterströmen von 640×360 bis 768×432: 60 Kameras brauchen rund 2,3 Kerne, im schlimmsten Fall mit ständiger Bewegung rund 2,9 Kerne bei 1,8 Bildern pro Sekunde. Unterströme mit 720p und 30 Bildern kosten beim Decodieren rund das Dreifache, deshalb je Kamera den kleinsten Unterstream wählen. An Kameras mit dem Schalter „Ablage nicht sichtbar“ rechnet für eine Person allein im Bild zusätzlich das größere Skelett-Modell (gemessen am Prüfrechner auf einem Kern: 38 bis 60 Millisekunden je Skelett statt 10 bis 22, bei drei Bildern je Sekunde also rund ein Achtel bis ein Fünftel eines Kerns je solcher Kamera); es teilt sich den festen Rechenpool, bei Andrang sinkt also auch dort nur die Bildrate. Geladen wird es erst, wenn eine solche Kamera es braucht.

Grenzen: - Die Person muss mit dem Oberkörper im Bild sein (eine Schulter und der Arm bis zum Ellbogen genügen) und mindestens ein Fünftel der Bildhöhe einnehmen. Kleinere Personen, etwa Passanten im Hintergrund, beobachtet die Wache nicht. Direkt vor der Kamera funktioniert es nicht. - Ohne Hüfte im Bild erkennt die Wache den Griff an Hosentasche und Bund nicht, nur das Verschwinden der Hand. Verschwindet die Hand hinter dem Vordergrund, gibt es einen Hinweis nur mit dem Schalter „Ablage nicht sichtbar“: wenn die Hand danach wieder im Bild und ohne Ware zu sehen ist, oder wenn

sie nicht wiederkommt und die Person allein im Bild war und es verlässt (Abgang). Ohne den Schalter bleibt es an solchen Kameras meist still. - Beim Abgang sehen Kunde und Dieb gleich aus: Den Hinweis löst auch aus, wer Ware nimmt, die Hand senkt und weitergeht. Das Skelett-Modell findet eine sichtbare Hand an solchen Kameras nicht in jedem Bild, „nicht mehr gesehen“ heißt also nicht immer „verdeckt“. Im normalen Verkaufsraum werden die meisten dieser Hinweise unbegründet sein; der Schalter ist für einzelne Kameras gedacht. Er wirkt nur, solange eine Person allein im Bild ist: Im vollen Laden bleibt der eigene Auslöser still. - Der Abgang steht erst fest, wenn die Personensuche zweimal in Folge niemanden findet, im Takt der Kamera-KI also fünf bis zehn Sekunden nach dem Weggehen; mit der Prüfung der Bild-KI kommt der Hinweis rund eine halbe Minute danach. Übersieht die Suche eine Person zweimal in Folge, gilt sie als gegangen. - Der eigene Auslöser und der Abgang sind an zwei Aufnahmen einer Person an einer Kamera geprüft (16. und 17.11.2026), dazu an zwei Aufnahmen mit voller Sicht und zehn Gegenproben einer Außenkamera. An einer laufenden Kamera ist der Abgang noch nicht ausgelöst worden. - Die Schätzung des Rumpfs stammt aus Aufnahmen einer einzigen Person an zwei Kameras. Sie lag dort bei 80 von 100 Skeletten höchstens 9 % neben der Messung; bei anderen Körpermaßen und Blickwinkeln kann sie weiter danebenliegen. - Von der Seite meldet das Skelett zeitweise beide Handgelenke an derselben Stelle. Die Wache behandelt ein Handgelenk, das zuletzt auf dem anderen lag und allein wegfällt, nicht als verschwundene Hand. Halten beide Hände die Ware eng zusammen und sinkt nur eine, bleibt das deshalb still. - Wer Ware einsteckt und die Hand danach mehrere Sekunden in der Tasche lässt, kann durchrutschen. Die Wache meldet lieber selten und dafür begründet. - Die Erkennung hängt vom Kamerawinkel ab. Liegt die Hand auf dem Weg unter die Kleidung außerhalb der Körpermitte, etwa seitlich am Kragen, bleibt der Griff ohne Hinweis. - Die Bild-KI beschreibt leere Hände manchmal als kleinen Gegenstand, deshalb zählen vage Beschreibungen nicht. Ein Griff in die Tasche ohne sichtbare Ware bleibt ohne Hinweis. - Der Rahmen „Gegenstand“ folgt der Spur der Person. Tritt binnen rund 15 Sekunden jemand anderes an dieselbe Stelle, kann er bis zum Ablauf der 60 Sekunden an dessen Hand erscheinen, ebenso nach dem Zurückstellen in eine Regalzone. Ein Hinweis entsteht daraus nicht. - Hält die Wache an, weil eine Freigabe entzogen wurde oder abgelaufen ist, bleiben gemerkte Einträge unerreichbar im Arbeitsspeicher liegen, bis der Dienst neu startet. - Die Fehlalarmquote im Ladenbetrieb ist noch nicht gemessen. - Die Bild-KI prüft auf dem Pentium rund 10 Griffe pro Minute. Bis zu drei Griffe je Kamera warten, weitere verfallen. Ob das im vollen Markt reicht, zeigt erst der Test.

Modell: MoveNet SinglePose Lightning (Apache-2.0), umgewandelt nach ONNX, aus dem Projekt von Kazuhito Takahashi. Für den eigenen Auslöser der Kameras mit „Ablage nicht sichtbar“ zusätzlich MoveNet SinglePose Thunder 4 (Apache-2.0, Eingang 256 × 256), aus dem SavedModel von TF-Hub mit tf2onnx nach ONNX umgewandelt (`models/movenet_thunder.onnx` , rund 25 MB). Die Wache liest die Eingangsgröße aus dem Modell; fehlt die Datei oder lässt sie sich nicht laden, rechnet auch der eigene Auslöser mit Lightning.

11. Meldungen

Seite Benachrichtigungen, „Kanal hinzufügen“. Jeder Kanal hat einen Test-Knopf, der Verlauf zeigt jede Meldung.

Einstellungen je Kanal

Einstellung	Bedeutung
Auslöser	Bewegung, KI-Erkennung, Zonen-Alarm, Prüfhinweis, Griff-Hinweis, Verhaltens-Erkennung, Bon nicht eingelöst, Störung, Kamera-Ereignis
Kameras	Mindestens eine
Cooldown	Mindestabstand zwischen zwei Meldungen
Zeitfenster	Außerhalb bleibt der Kanal stumm
Nur wenn Anlage scharf	Kanal schweigt im unscharfen Zustand, Störungen sind ausgenommen

> Empfehlung für den Handel: Nur **Prüfhinweis** und **Störung** als Auslöser. „Nur wenn Anlage scharf“ aus, sonst kommen Hinweise während der Öffnungszeiten nicht an. Bewegung und KI lösen bei jedem Kunden aus.

> Für Störungsmeldungen braucht der Kanal den Auslöser Störung. Meldungen zu Speicher, KI und Stream-Dienst gehen auch an Kanäle mit Kamera-Teilauswahl. Zeitfenster und Cooldown gelten auch für Störungen.

> Bestehende Kanäle behalten ihre Auslöser. Neue Kanäle sind im Datenschutzprofil auf Prüfhinweis und Störung vorbelegt, ein neuer Leitstellen-Kanal immer auf Zonen-Alarm. Speichern Sie nach jeder Änderung.

Zugangsdaten im Kanal: Beim Ansehen zeigt die Oberfläche Webhook-, Teams- und API-Adressen nur mit Host, Schlüssel und Passwörter nur mit den letzten 4 Zeichen. Gespeichert bleiben die vollen Werte, eine neue Adresse tragen Sie vollständig ein.

Push mit ntfy: Server, Token und Topic sind vorbelegt. Der Dialog zeigt unter „Handy einrichten“ die Zugangsdaten für die App. Im Datenschutzprofil gibt es ohne Freigabe kein iOS-Wecksignal, Push ist dort vor allem für Android belastbar.

Link in der Meldung: Bei ntfy und E-Mail öffnet ein Tipp das Ereignis. Der Link entsteht nur mit aktivem Fernzugriff oder gesetzter Öffentlicher Basis-URL unter Einstellungen, Verbindungen.

Vorschaubild: Ohne Datenschutzprofil schicken die Kanäle das Ereignisbild mit, wie sie es können. Im Profil gehen Meldungen ohne Bild hinaus. Mit der Freigabe „Vorschaubild in E-Mail und Push“ geht bei KI-Erkennung und Zonen-Alarm ein Vorschaubild mit, verpixelt wie das Prüfbild: Köpfe der erkannten Personen und Gesichter, bei Fahrzeugen der untere Teil, wo in der Regel das Kennzeichen sitzt, beim Motorrad das ganze Fahrzeug. Kleidung bleibt erkennbar. Zum Verpixeln berücksichtigt LocalEye alle Personen und Fahrzeuge, die die KI im Bild erkennt, auch außerhalb der Zonen und unabhängig von der

Objektauswahl der Kamera. So wird auch bei parkenden Autos der untere Teil verpixelt, wenn die Kamera nur Personen zählt. Prüfhinweise, Griff-Hinweise, Verhaltens-Erkennung, Bewegung und Kamera-Ereignisse bleiben ohne Bild. Klappt das Verpixeln nicht oder fehlt eine gültige Box einer Person oder eines Fahrzeugs, geht kein Bild hinaus. Jeder Versand steht im Journal („Vorschaubild verpixelt an einen Meldekanal übergeben“, je Kanal und Kamera höchstens einmal in 10 Minuten, ohne Empfänger).

> Der Push-Dienst ist nicht über den Fernzugriff erreichbar. Für Push außerhalb des lokalen Netzes muss der Server per Reverse-Proxy oder VPN erreichbar sein und seine Adresse unter Einstellungen, Verbindungen eingetragen werden. Sonst nutzen Sie E-Mail.

Scharf und unscharf: Der Knopf in der Seitenleiste schaltet um, das Uhr-Symbol daneben öffnet den Zeitplan. Der Zustand steuert nur Kanäle mit „Nur wenn Anlage scharf“. Aufnahme und Erkennung ändern sich dadurch nicht.

Stummschalten: Der Schalter „Meldungen aktiv“ / „Stummgeschaltet“ auf der Seite Benachrichtigungen betrifft alle Meldekanäle außer der Leitstelle (Push, E-Mail, Teams, Webhook, Messenger). Die Leitstelle bleibt aufgeschaltet; wer im Objekt arbeitet, schaltet unscharf. Fehlt die Option „Nur wenn Anlage scharf“ an einem aktiven Leitstellen-Kanal, steht am Schalter: „Der Leitstellen-Kanal meldet auch unscharf: Option „Nur wenn Anlage scharf“ am Kanal einschalten.“ War die Anlage beim Update stummgeschaltet, gilt diese Stummschaltung bis zum nächsten Aufheben auch für die Leitstelle. Hat die Anlage einen aktiven Leitstellen-Kanal, steht solange im Störungsbanner der Seitenleiste „Meldungen stummgeschaltet, auch die Leitstelle“. Danach lässt jede neue Stummschaltung die Leitstelle aus.

12. Fernzugriff

Voraussetzungen - Lizenz aktiv und Einrichtung abgeschlossen - Ausgehend TCP 7000 frei, ohne SSL-Inspection - Im Datenschutzprofil: alle Admins mit 2FA

Der Fernzugriff richtet sich selbst ein und wird jede Minute abgeglichen. Fällt eine Bedingung weg, stoppt er von selbst.

Anmelden 1. `https://remote.localeye.shop/remote` öffnen. 2. Mit dem Lizenzschlüssel anmelden, mit eingerichtetem zweiten Faktor zusätzlich mit Code. 3. Standort öffnen. 4. In LocalEye mit dem persönlichen Konto anmelden.

Sitzung: Die Portal-Anmeldung gilt 12 Stunden und verlängert sich nicht. Danach ist eine neue Anmeldung nötig, auch während laufender Arbeit.

Von außen erreichbar: Live-Video, Aufnahmen, Snapshots, Einstellungen je nach Rolle.

Von außen gesperrt: „Anlage verwalten“, Zusatz-Apps, Kameras und NVR direkt, das übrige Netz, die NVR-Daueraufzeichnung, die Ansicht `/leitstelle/` für Konten der Rolle Leitstelle. Im Datenschutzprofil zusätzlich alle Admin-Funktionen der Oberfläche samt Einstellungen, Benutzern und Meldekanälen.

> Admins können über den Fernzugriff Funktionen auslösen, die im lokalen Netz wirken, etwa Netzwerk-Scan, Kamera-Test und die Verwaltung des Stream-Dienstes. Im Datenschutzprofil sperrt die Anlage alle Admin-Funktionen über den Fernzugriff. Schützen Sie jedes Admin-Konto mit 2FA.

> Richten Sie im Portal den zweiten Faktor ein. Danach reicht der Lizenzschlüssel allein nicht mehr. Die acht Wiederherstellungs-Codes sicher ablegen.

Mehrere Standorte: Mehrere Märkte unter einem Schlüssel erscheinen automatisch. Standorte mit eigenem Schlüssel nehmen Sie im Portal unter „Standort hinzufügen“ dazu.

Abschalten: „Anlage verwalten“, Karte Fernzugriff, Schieberegler. Wieder einschalten geht nur im lokalen Netz. Als Alternative erreichen Sie die Anlage über ein eigenes VPN.

> Beim Fernzugriff läuft das angezeigte Video durch das Relay. Dort wird es im Durchlauf entschlüsselt und nicht gespeichert. Es ist keine Ende-zu-Ende-Verschlüsselung. Dafür ist ein Auftragsverarbeitungsvertrag nötig.

13. Aufnahmen, Fristen und Nachweise

Aufnahme: An die KI gekoppelt. Eine Erkennung löst Snapshot und Video aus. Der Pre-Roll fügt bei Kameras über go2rtc Sekunden davor hinzu, UniFi-Protect-Kameras haben keinen. Das Zeichen „⏪ +Xs“ an der Aufnahme zeigt die tatsächlich vorangestellte Vorlauf-Länge in Sekunden, gemessen an den angefügten Segmenten. Direkt nach dem Start einer Kamera kann sie kürzer sein als eingestellt. Aufgenommen wird der Haupt-Stream, bei Kameras mit wenigen Verbindungen der Sub-Stream. Eine KI-Aufnahme läuft, solange eine Person im Bild ist, höchstens 10 Minuten je Datei, danach beginnt bei der nächsten Meldung eine neue. Manuelle Aufnahmen enden im Datenschutzprofil nach höchstens 2 Stunden von selbst.

Liste: Die Seite Aufnahmen zeigt je Abschnitt die neuesten 200 Aufnahmen. „Ältere Aufnahmen laden“ unter der Liste holt den nächsten Abschnitt; ein gewählter Kamerafilter gilt dabei weiter. Sind ältere Abschnitte nachgeladen, bleibt die Liste nach Legal Hold, Freigeben oder Löschen stehen. Lehnt die Anlage dann ein Löschen ab (zum Beispiel, weil die Aufnahme noch läuft oder inzwischen unter Legal Hold steht), nennt eine Meldung den Grund.

Fristen: Einstellungen, Speicher. Getrennt für Aufnahmen, Snapshots und Meldungs-Verlauf, 0 bedeutet nie löschen. Der Meldungs-Verlauf löscht ab Werk nach 30 Tagen.

Legal Hold: In der Aufnahmen-Liste „Hold“ mit Begründung setzen. Weder Löschen-Knopf noch automatischer Lauf entfernen die Aufnahme. Der automatische Lauf lässt außerdem Bilder, Berichte und Indexzeilen derselben Kamera aus dem Zeitraum der Aufnahme stehen, mit zwei Minuten Rand, auch von Hand ausgelöste Snapshots. Dazu gehören die Ereignisbilder der Meldungen, die an einem Bericht aus diesem Zeitraum hängen, auch das des Zonen-Alarms samt Prüfclip.

Beweispaket: Lädt eine ZIP mit Video, Manifest mit SHA-256, Prüfwert der Anlage und dem Skript `PRUEFEN.py`. „Paket prüfen“ auf der Aufnahmen-Seite bestätigt die Herkunft.

Protokoll: Einstellungen öffnen, dann unter System „Protokoll“. Das Audit-Journal hält Anmeldungen, angesehene und gelöschte Aufnahmen, Snapshot-Ansichten, Exporte samt Excel-Export des Meldungsverlaufs, jeden Aufruf von Prüfseite und Prüfbild (Obergrenze gegen Fluten: 30 Einträge je Art und Ereignis in einer Minute), Bewertungen von Prüfhinweisen und ihr Aufheben, Einstellungs- und Benutzeränderungen, Freigaben im Datenschutzprofil, Live-Ansichten (je Nutzer und Kamera höchstens ein Eintrag in 10 Minuten, Live-Video einer Erweiterung auf der Hauptanlage mit Standort und Quelle, im Datenschutzprofil auch das Einzelbild: Kachel, Vollbild, Kacheln einer Erweiterung und des Leitstands, das Protect-Einzelbild und der Abruf unter `/api/snap/` mit Anmeldung), Scharf und Unscharf sowie Löschläufe fest. Die Einträge der Leitstellen-Ansicht („Leitstelle abgewiesen“, „Leitstellen-Ansicht geöffnet“, „Leitstelle: Ereignis angesehen“, „Leitstelle: Prüfbild abgerufen“) gibt es mit und ohne Datenschutzprofil. Im Profil kommen unter anderem „Abruf per Token abgelehnt“, „Token entfernt“, „Verwaltung abgewiesen“, „Vorschaubild einer Aufnahme angesehen“, „Vorschaubild verpixelt an einen Meldekanal übergeben“, „Lernlauf abgelehnt“, die Sicherungen samt Frist und Zurückspielen und je Stunde die Zahl verworfener Kamera-Ereignisse dazu. Filter und Excel-Export sind vorhanden. Aufbewahrung Vorgabe 365 Tage unter Einstellungen, Verbindungen.

> „Kette prüfen“ erkennt geänderte oder herausgelöste Einzeleinträge. Abgeschnittene Enden, ein Restore oder eine neu berechnete Kette erkennt erst der Abgleich mit einer externen Kopie. Exportieren Sie das Protokoll deshalb regelmäßig.

14. Updates

Ab Werk startet kein Update von selbst.

Online: „Anlage verwalten“, Karte Update, „Jetzt aktualisieren“. Die Anlage holt die Version mit dem Lizenzschlüssel aus dem Shop und prüft danach alles mit dem Selbsttest.

Per Datei: In derselben Karte unter „Release-Datei hochladen“ die Datei wählen und „Hochladen und einspielen“ klicken, oder `./manage.sh update <zip>`. Kamera-Erweiterungen aktualisieren Sie immer per Datei. Im Verbund aktualisieren Sie alle Maschinen im selben Wartungsfenster. Ohne Datenschutzprofil zuerst die Erweiterungen, dann die Hauptanlage. Im Datenschutzprofil umgekehrt, zuerst die Hauptanlage, siehe Kapitel Verbund.

> Ab Version 2026.11.16 ist die Kennzeichenerkennung entfernt. Der erste Start nach dem Update löscht ihre gespeicherten Daten, siehe Kapitel EDEKA-Betrieb. Im Datenschutzprofil braucht ab dieser Version jede Sicherung ein Sicherungs-Passwort, auch die Sicherheitssicherung vor einem Zurückspielen. Setzen Sie es vor dem Update.

Ablauf 1. Die Anlage prüft Signatur und jede Datei. Seit dem ersten signierten Release lehnt sie veränderte, unsignierte und ältere Pakete ab. 2. Dienste werden neu gebaut und gestartet, laufende Aufnahmen pausieren kurz. 3. Daten, Kameras und Einstellungen bleiben erhalten. 4. Installiert ein Update den NVIDIA-Treiber, bietet es den Neustart erst ganz am Ende an, beim Online-Update nach dem Selbsttest.

> Lange Aufträge laufen auf dem Gerät weiter, auch wenn der Browser zugeht. Die Seite findet den Auftrag danach wieder.

Prüfen Sie nach jedem Update den Status oder führen Sie `./manage.sh selbsttest` aus. Ein Rückschritt auf eine ältere Version ist nur mit dem Hersteller vorgesehen.

> Scheitert der Bau, laufen die alten Dienste weiter, nginx und die Verwaltung sind dann schon neu. Laden Sie die Release-Datei für den zweiten Versuch erneut hoch und haken Sie „Vollständig neu bauen (--no-cache)“ an. Online meldet die Anlage danach „aktuell“. Scheitert erst der Start der neuen Dienste, gibt es keinen automatischen Rückweg, wenden Sie sich an den Hersteller.

15. Sicherung und Wiederherstellung

Sichern: „Anlage verwalten“, Karte Sichern. Ziele: lokal, ein Ordner auf dem Gerät wie eine USB-Festplatte, SMB oder NFS. Die Anlage behält 15 eigene Sicherungen (`BACKUP_ZIEL_BEHALTEN`); Sicherungen anderer Anlagen am selben Ziel zeigt die Karte nicht und löscht sie nie.

Inhalt: Konfiguration samt Zugangsdaten, Snapshots, KI-Berichte, Zusatz-App-Daten. Aufnahmen sind nicht enthalten, im Datenschutzprofil auch keine Snapshots und KI-Berichte.

Sicherungs-Passwort: In der Karte Sichern unter „Sicherungs-Passwort“ oder mit `./manage.sh sicherung-passwort` legen Sie ein Passwort fest. Damit werden neue Sicherungen verschlüsselt und lassen sich auch auf einem Ersatzgerät prüfen und einspielen. Ohne dieses Passwort ist eine verschlüsselte Sicherung nicht wiederherstellbar, bewahren Sie es also getrennt von der Anlage auf. Ein neues Passwort gilt für neue Sicherungen; ältere brauchen ihr bisheriges. Liegt das Ziel im Netz und ist kein Passwort gesetzt, warnt die Karte. Verschlüsselt wird nur, wenn auf dem Gerät openssl ab Version 1.1.1 vorhanden ist. Ohne Datenschutzprofil gilt: Fehlt es oder ist es älter, entstehen Sicherungen trotz Sicherungs-Passwort unverschlüsselt; die Karte Sichern und der Selbsttest weisen darauf hin. Wer eine Sicherung entschlüsseln kann, hat alles, was darin liegt: Konten samt Geheimnissen des zweiten Faktors, die `.env` und die Schlüssel der Kopplung im Verbund. Schützen Sie das Passwort wie den Zugang zur Anlage selbst.

Sicherungen im Datenschutzprofil: Ohne gültiges Sicherungs-Passwort entsteht keine Sicherung, auf keinem Weg: weder mit `./manage.sh backup` noch in der Karte Sichern noch als Sicherheitssicherung vor dem Zurückspielen. Damit bricht auch das Zurückspielen ab, ohne etwas zu verändern. Fehlt openssl ab Version 1.1.1, bricht die Sicherung ebenso ab. Setzen Sie das Passwort deshalb vor der ersten Sicherung. In „Anlage verwalten“ verlangen das Ändern und das Entfernen des Passworts und jede Änderung des Sicherungsziels den Code aus der Authenticator-App oder einen Wiederherstellungs-Code; das erste Setzen und unverändertes Speichern gehen ohne. Am Terminal entfernt `sudo ./manage.sh sicherung-passwort entfernen` das Passwort ohne zweiten Faktor, der Eintrag steht vorher im Journal. Setzen und Entfernen, die Rotation und ein Wechsel des Sicherungsziels stehen im Journal. Bricht eine Sicherung ab, bleibt keine unverschlüsselte Arbeitskopie liegen.

Frist der Sicherungen im Datenschutzprofil: `SICHERUNG_FRIST_TAGE` in der `.env` legt fest, nach wie vielen Tagen die Anlage ihre eigenen Sicherungen löscht. Leer heißt 7, gültig ist eine ganze Zahl von 1 bis 9999. Gelöscht wird nach dem Zeitstempel im Namen, nur echte Dateien direkt im Sicherungsordner, mit Eintrag im Journal vor dem Löschen. Das tun jede neue Sicherung und ein täglicher Fristlauf, den „Anlage verwalten“ selbst anstößt, erstmals zehn Minuten nach dem Start und nie während eines laufenden Auftrags. Einen cron-Eintrag braucht es nicht, von Hand geht es mit `sudo ./manage.sh sicherung-frist` . Ein ungültiger Wert löscht nichts und ist im Selbsttest ein Fehler. Ist der Fristlauf nie gelaufen oder älter als 48 Stunden, meldet der Selbsttest einen Fehler und die Abnahme eine ABWEICHUNG. An einem Netzziel (SMB, NFS) wirkt die Frist bei jeder Sicherung und beim Fristlauf.

> Die Frist rechnet mit der Uhr der Anlage. Springt die Uhr um mehr als die Frist nach vorn, löscht der Fristlauf alle Sicherungen, auch die jüngste. Schützen Sie deshalb die Zeitquelle der Anlage (NTP). Ein Papierkorb der Netzfreigabe liegt außerhalb der Anlage. Sicherungen einer Vorgänger-Anlage am selben Ziel löscht die Frist nicht, nach einem Gerätetausch löschen Sie diese von Hand.

Legal Hold und Sicherung: Im Datenschutzprofil kommt gehaltenes Material nicht in die Sicherung, dort steht nur der Eintrag im Journal. Es liegt nur auf der Anlage. Laden Sie zu jedem Hold das Beweispaket

herunter und geben Sie es der zuständigen Stelle, dann übersteht der Beweis einen Geräteausfall.

> Ohne Sicherungs-Passwort sind Sicherungen unverschlüsselt und enthalten Zugangsdaten, im Datenschutzprofil entsteht dann gar keine. Legen Sie sie nur geschützt ab. Die Daten auf der Anlage selbst sind nicht verschlüsselt, das Gerät gehört in einen verschlossenen Raum.

Echtheitsnachweis: Jede Sicherung trägt ein Anlagenkürzel im Namen und einen Echtheitsnachweis (Datei `.nachweis` daneben). In der Karte Zurückspielen lassen sich nur Sicherungen mit gültigem Nachweis einspielen. Der Echtheitsnachweis gilt für genau den Dateinamen der Sicherung: Eine umbenannte Sicherung gilt nicht mehr als echt. Sicherungen einer anderen Anlage lassen sich nur am Terminal einspielen und brauchen dort die getippte Bestätigung „ANDERE ANLAGE“.

Sicherungsziel: Ein eigener Ordner oder eine Freigabe behält seine Rechte; die Sicherungsdateien selbst sind nur für root lesbar. Wer im Zielordner schreiben darf, kann Sicherungen dort löschen; ein Austausch fällt beim Einspielen am Echtheitsnachweis auf. „Speichern und prüfen“ hängt die Freigabe immer selbst ein. Läuft gerade eine Sicherung auf dieselbe Freigabe, wartet die Prüfung bis zu einer Minute und meldet dann, dass das Sicherungsziel belegt ist. Ebenso wartet eine zweite Sicherung bis zu einer Minute und bricht sonst mit dieser Meldung ab. Während eine Sicherung läuft, liegt sie in einem Arbeitsordner `.allinone-sicherung-…` im Ziel und erscheint erst fertig in der Liste. Bleibt nach einem Abbruch ein solcher Ordner liegen, entfernt ihn die nächste Sicherung nach 24 Stunden.

Sicherungen von vor dem Update: Sicherungen von vor dem Update im Ordner `backups/` bekommen ihren Echtheitsnachweis einmalig bei der ersten Sicherung oder beim ersten Zurückspielen nach dem Update. Bis dahin tragen sie in der Karte das Kennzeichen „Nachweis folgt“. Später in den Ordner kopierte Sicherungen ohne Nachweis lassen sich nur am Terminal nach Bestätigung einspielen. Sicherungen im alten Namensformat an einem Sicherungsziel außerhalb (Ordner, Freigabe) räumt die Anlage nach dem Update nicht mehr automatisch auf, weil sie dort nicht sicher zu ihr gehören. Die Karte Sichern nennt ihre Anzahl und Gesamtgröße; bei knappem Platz bitte von Hand am Ziel löschen.

Zurückspielen: Karte Zurückspielen. Alle seither entstandenen Daten gehen verloren. „Mit Einstellungen“ ersetzt zusätzlich `.env` und Zugangsdaten, im Datenschutzprofil bleibt die `.env` der Anlage stehen. `docker-compose.yml` und `nginx.conf` bleiben auf dem installierten Stand; die gesicherte Fassung liegt als `*.aus-sicherung-<zeit>` daneben.

Zurückspielen im Datenschutzprofil: Mit Einstellungen (`--with-config`) bleibt die `.env` der Anlage stehen, aus der Sicherung kommt kein Wert. Das Protokoll des Auftrags nennt nur die Namen der Schlüssel, die die Sicherung anders oder allein hat, nie Werte. Wer einen davon braucht, trägt ihn von Hand ein. Die Abschalt-Freigabe kommt nicht aus der Sicherung. Eine Gegenprobe prüft vorher, dass das Profil danach weiter gilt, sonst wird nicht zurückgespielt. Es bleiben außerdem die Kopplung im Verbund, die Vorgabe der Hauptanlage, die Aufbewahrungsdauer des Journals und der Ordner `localeye/go2rtc`. Freigaben und Schalter kommen wie in der Sicherung; der Journaleintrag „zurückgespielt“ nennt die Freigaben, die dadurch wieder gelten. Das Journal wird weitergeführt, wenn die Sicherung von dieser Anlage stammt. Ein Ersatzgerät mit junger eigener Kette bekommt das Journal der Sicherung, seine eigenen Einträge hängen danach mit Vermerk ihrer Herkunft an. Ist die Lage unklar, wird nicht zurückgespielt, die Meldung nennt den Weg. Konfiguration, Konten und Zugang des Push-Dienstes kommen auch im Profil aus der Sicherung. Spielen Sie deshalb keine Sicherung aus fremder Hand zurück.

Zurückspielen am Terminal: `sudo ./manage.sh restore <datei>` prüft zuerst den Echtheitsnachweis. Fehlt er oder passt er nicht (z. B. Sicherung von vor dem Update), geht das Einspielen nur am Terminal

nach Eingabe von `UNGEPRUEFT`, mit `--with-config` zusätzlich `KONFIGURATION`. Fehlt einer verschlüsselten Sicherung der Echtheitsnachweis, fragt das Zurückspielen am Terminal nach ihrem Sicherungs-Passwort (Eingabetaste nimmt das gespeicherte) und prüft es sofort. Nach drei falschen Versuchen endet es, ohne etwas zu verändern.

Ersatzgerät: Nach der Neuinstallation dasselbe Sicherungsziel eintragen. Die Sicherungen der ausgefallenen Anlage zeigt `sudo ./manage.sh restore ziel:` an; die Karte Zurückspielen zeigt sie nicht. Eingespielt wird mit `sudo ./manage.sh restore ziel:<datei>`, dem Sicherungs-Passwort und der Bestätigung „ANDERE ANLAGE“. Wurde ohne Sicherungs-Passwort gesichert, kann das Ersatzgerät den Echtheitsnachweis nicht prüfen; dann verlangt das Einspielen zusätzlich „UNGEPRUEFT“.

Kopierte Installation: Wird ein Installordner kopiert und mit anderem `INSTANCE_SUFFIX` betrieben, gilt die Kopie als eigene Anlage: Bei ihrer ersten Sicherung bildet sie ein eigenes Kürzel und einen eigenen Geräteschlüssel. Die mitkopierten Sicherungen der Quelle zählen dort als Sicherungen einer anderen Anlage. Dasselbe geschieht, wenn das `INSTANCE_SUFFIX` einer Anlage nachträglich geändert wird.

Empfehlung: Sichern Sie auf ein anderes Gerät als die Anlage und testen Sie das Zurückspielen einmal vor dem Echtbetrieb.

Verbund: Jede Erweiterung sichert ihre Konfiguration automatisch zur Hauptanlage. Ein Ersatzgerät übernimmt Kameras, Einstellungen und Meldenummern.

16. Überwachung und Diagnose

Anlagenwächter: Prüft jede Minute Kamerabilder, Speicher, KI-Modell, Stream-Dienst und Leitstellen-Meldungen, bei eingeschalteten Prüfhinweisen auch die Bild-KI, ohne Prüfhinweise dann, wenn die Bildbeschreibung an ist und der Bildserver auf diesem Gerät laufen soll. Nach drei Treffern in Folge meldet er eine Störung, nach zwei guten Durchläufen die Entstörung.

- Ein gelbes Banner in der Seitenleiste nennt die Störung im Klartext.
- Damit Störungen verschickt werden, muss ein Kanal den Auslöser Störung haben.
- Schwellen unter Einstellungen, Verbindungen, Vorgabe 120 Sekunden Bildalter und 5 GB Speicher.
- „Ereignisquelle der Kamera „Name“ abgelehnt: Zugangsdaten prüfen“: Die Kamera hat die Anmeldung der Ereignisquelle abgelehnt. LocalEye versucht es nicht erneut, damit die Kamera nicht sperrt. Nach dem Ändern der Zugangsdaten verbindet es neu und die Störung endet.
- „Bild-KI antwortet nicht — Ereignisse bekommen keine Beschreibung“: Der Bildserver soll auf diesem Gerät laufen, antwortet aber nicht. Ereignisse werden ohne Beschreibung gespeichert, die Recherche in KnowSora findet sie dann nicht über den Bildinhalt. Diese Störung geht nicht an die Leitstelle.

Monitoring-Systeme: `/metrics` liefert Kennzahlen je Kamera und Anlage, Zugriff mit API-Token im Kopf `X-API-Token` oder als angemeldeter Admin.

Selbsttest: `./manage.sh selbsttest` prüft Dienste, Weboberfläche, HTTPS samt `LAN_HTTP`, Modelle, Relay, Signatur und Speicher. Direkt nach einem Update kann eine Warnung erscheinen, weil Dienste noch starten. Dann wiederholen. Mit `LAN_HTTP=aus` und wirksamem Datenschutzprofil meldet der Selbsttest nach abgeschlossener Einrichtung einen Fehler, wenn HTTP aus dem Netz mit etwas anderem antwortet als der Umleitung auf HTTPS oder dem Schließen der Verbindung, oder wenn HTTPS nicht eingerichtet ist bzw. nicht antwortet. Während der Einrichtung und ohne Profil bleiben das Warnungen. Findet die Anlage keine Netzadresse, steht „HTTP-Sperre nicht geprüft“ als Warnung da. Der Selbsttest hat den Abschnitt „Sicherung“. Liegt das Sicherungsziel im Netz und entstehen die Sicherungen unverschlüsselt, warnt er: „Sicherung am Netzziel unverschlüsselt: Sicherungs-Passwort setzen“. Im Datenschutzprofil zeigt er zusätzlich: Kamerabilder über Token gesperrt, den Adressbereich der Verwaltung (leer ist ein Hinweis, ungültig ein Fehler, sehr weite Bereiche eine Warnung), die gemessene Bindung von go2rtc, Sicherungs-Passwort, Fristlauf und Sicherungen älter als die Frist, den Stand des Lernlaufs und die Zahl der verworfenen Kamera-Ereignisse mit dem Stand der letzten vollen Stunde.

Meldungen des Selbsttests zur KI-Sandbox und zum Sandkasten von KnowSora: - „KI-Sandbox laeuft privilegiert“: Bestehende Anlage, die Sandbox läuft noch mit einem Docker-Daemon als root. Beheben mit `./manage.sh ki-sandbox absichern`. Steht dabei „Image der abgesicherten Art liegt nicht vor und die Image-Quelle ist nicht erreichbar“, hat das Gerät kein Internet und das Image fehlt. Mit Internet `./manage.sh ki-sandbox absichern` ausführen. - „Docker-API der KI-Sandbox antwortet im Netz des Hosts“: Der Docker-Daemon der KI-Sandbox lauscht zusätzlich auf einem Netz-Port (2375 oder 2376). Das Update stellt den Dienst `knowsora-ai-dind` in der `docker-compose.yml` um. Findet es dort die erwartete Startzeile nicht, weil die Datei von Hand geändert wurde, bleibt der Port offen. Das Update erneut einspielen. Bleibt die Meldung, den Dienst `knowsora-ai-dind` in der `docker-compose.yml` mit der `docker-compose.yml.example` vergleichen, die Zeile mit `dockerd-entrypoint.sh` von dort übernehmen und `./manage.sh restart` ausführen. Die Warnung „nicht pruefbar, ob sie im Netz des Hosts erreichbar ist“ heißt: Der Container der KI-Sandbox hat keine eigene Adresse oder auf dem Gerät fehlt `python3`; dann dieselbe Zeile von Hand mit der Vorlage vergleichen. - „Netzregeln nicht verfügbar“: Der Kernel kann Netzregeln für den Sandkasten nicht setzen (vor 6.7). KI-Läufe erreichen die Dienste der Plattform

weiterhin. - „Claude-Haken der verwalteten Vorlage rufen Dateien auf, die jede Shell-Sitzung in KnowSora ändern kann“: Das genannte Skript an einen Ort legen, den KI-Läufe nicht beschreiben können, und den Pfad in der Vorlage ändern, oder den Haken entfernen.

Protokolle: „Anlage verwalten“, Karte Betrieb, Dienst-Log, oder `./manage.sh logs`.

17. Verbund und Leitstelle

Verbund

Der Verbund verteilt Kameras auf eine Hauptanlage und Kamera-Erweiterungen. Erweiterungen laufen autonom weiter, wenn die Hauptanlage ausfällt.

1. Erweiterung mit gleicher Release-Version installieren, Betriebsart Kamera-Erweiterung, Adresse der Hauptanlage eingeben.
2. Nach dem ersten Start `./manage.sh join` ausführen, die Konsole zeigt einen Prüfcode.
3. In der Hauptanlage unter Verbund Code vergleichen und bestätigen.

Soll die Hauptanlage die Erweiterung über „Erweiterung hinzufügen“ einladen, braucht sie deren Einmalcode: `./manage.sh kopplungscode` auf der Erweiterung zeigt ihn an. Er gilt 30 Minuten und für genau einen Versuch, danach zeigt der Befehl einen neuen. Fünf falsche Codes sperren die jeweilige Adresse für 15 Minuten. Eine Erweiterung gibt Konten ohne zweiten Faktor keine Verwaltungssitzung, solange sie gekoppelt ist. Scheitert die Einladung, nachdem die Erweiterung den Kopplungscode angenommen hat, ist der Code verbraucht. Lassen Sie auf der Erweiterung mit `./manage.sh kopplungscode` einen neuen anzeigen und wiederholen Sie die Einladung.

Im Datenschutzprofil gehen Koppeln, Trennen, Bestätigen, Entfernen, Einladen und das Lesen des Kopplungscodes per API-Token nur noch am Gerät, also mit `./manage.sh join` und `./manage.sh kopplungscode`. Von außen antwortet die Anlage mit 410 und schreibt „Abruf per Token abgelehnt“ ins Journal. Richten Sie vor dem Koppeln HTTPS ein (`LAN_HTTP=aus`): Eine Kopplung über HTTP lässt sich im LAN mitschneiden, daraus lässt sich der Schlüssel des Verbunds ableiten.

Benutzer, Kanäle und Einstellungen pflegen Sie zentral auf der Hauptanlage. Notzugang: `./manage.sh notfall-gui an` und `aus`.

Verbund im Datenschutzprofil: Nehmen Sie Hauptanlage und Erweiterungen beide ins Profil und halten Sie sie auf demselben Stand. Aktualisieren Sie zuerst die Hauptanlage, dann die Erweiterungen: Erst die neue Hauptanlage meldet im Abgleich, dass sie lesende Durchgriffe selbst prüft. Bis dahin lassen sich die Verwaltungs-Seiten einer schon aktualisierten Erweiterung über die Hauptanlage nicht öffnen. Läuft die Hauptanlage im Profil, prüft sie den Menschen mit ihrem eigenen Adressbereich, für Änderungen an der Erweiterung und für das Lesen ihrer Admin-Seiten (Journal, Meldekanäle, API-Token, KI-Kalibrierung). Über den Fernzugriff der Hauptanlage geht beides nie. Kameras, Aufnahmen und Ereignisse der Erweiterung lassen sich wie an der Hauptanlage selbst ansehen, auch von außerhalb des Bereichs. Läuft nur die Erweiterung im Profil oder hat die Hauptanlage eine ältere Fassung, ist die Verwaltung der Erweiterung über die Hauptanlage gesperrt, die Meldung beginnt mit „Verwaltung dieser Erweiterung über die Hauptanlage gesperrt“. Verwalten lässt sie sich dann nur über ihren Notzugang: am Gerät `./manage.sh notfall-gui an`, danach wieder schließen mit `./manage.sh notfall-gui aus`. Der Notzugang ist für den Notfall gedacht, nicht für den Dauerbetrieb. Im Journal der Erweiterung steht dann „Verwaltung abgewiesen“ mit dem Grund `hauptanlage_prueft_nicht` oder `hauptanlage_ohne_profil`. Läuft nur die Erweiterung im Profil, holt die Hauptanlage alle fünf Minuten den Recherche-Spiegel; das ergibt rund 288 solcher Einträge am Tag und ist kein Angriff.

Eigene Sperre der Erweiterung: `./manage.sh profil edeka` überträgt auf einer Erweiterung nichts, das Profil gibt die Hauptanlage vor. Ohne `PRIVACY_LOCK=edeka` in der `.env` der Erweiterung endet ihr Profil, wenn sie vom Verbund getrennt wird. Tragen Sie die Zeile deshalb von Hand ein, die Abnahme meldet

eine fehlende eigene Sperre als ABWEICHUNG. Den Adressbereich der Verwaltung legt jede Anlage selbst fest: Am Terminal bietet `./manage.sh profil edeka` auf der Erweiterung an, nur `VERWALTUNG_LAN_CIDRS` zu setzen.

Journal im Verbund: Ändert ein Admin der Hauptanlage eine Erweiterung über den Durchgriff oder holt er dort einen Export ohne Bilder, steht das im Journal der Erweiterung mit `verbund:<Kennung>`, nicht mit dem Menschen. Die Hauptanlage schreibt den Menschen bei Bildabrufen, beim KI-Bericht und beim Trennen.

Verwalten aus der Hauptanlage: Lehnt eine Erweiterung eine Aktion ab, zum Beispiel wegen des Datenschutzprofils, erscheint ihre Meldung und die Seite bleibt bei der Erweiterung. Zurück zur Hauptanlage führt nur eine abgelaufene Anmeldung oder ein fehlendes Admin-Recht. Hat eine Erweiterung einen älteren Stand als die Hauptanlage, zeigt ihre Seite Aufnahmen nur die neuesten 200 Aufnahmen; „Ältere Aufnahmen laden“ meldet das. Nach dem Update der Erweiterung lassen sich auch ältere nachladen.

Adresse der Hauptanlage ändert sich: Bekommt die Hauptanlage eine neue IP-Adresse, setzen Sie an jeder Erweiterung in der `.env` `FED_PARENT_URL` auf die neue Adresse, z. B. `http://192.0.2.10:8987`. Ändert sich der Verbund-TLS-Port, tragen Sie dort die https-Adresse mit dem neuen Port ein, z. B. `https://192.0.2.10:8443`. Die Erweiterung erreicht die Hauptanlage dann beim nächsten Heartbeat ohne neues Koppeln und prüft weiter das gemerkte Zertifikat der Hauptanlage.

> Die Uhren müssen stimmen. Ab 5 Minuten Abweichung werden signierte Nachrichten abgewiesen.

Leitstand

Der Leitstand zeigt mehrere eigenständige Anlagen rein lesend. Er braucht einen Netzweg zwischen den Anlagen, etwa ein VPN. Über das Relay läuft er nicht.

Eine Anlage im Datenschutzprofil liefert dem Leitstand anderer Anlagen weder Übersicht noch Kachelbild: Ihr Freigabe-Token bekommt 410. Ihr eigener Leitstand geht nur mit Anmeldung als Admin. Siehe Kapitel Datenschutzprofil, Zeile Token.

Leitstelle

Kanaltyp SIA DC-09 mit Primär- und Backup-Empfänger. Jede Kamera trägt eine dauerhafte Leitstellen-Nummer.

> SIA DC-09 läuft derzeit ohne AES-Verschlüsselung. Der Transport gehört in ein VPN oder Alarmnetz. Im Verbund überträgt die Hauptanlage alle Kanäle samt SIA-Kanal, eine eigene Anlagenkennung je Maschine gibt es nicht. Stimmen Sie SIA im Verbund mit dem Hersteller ab.

Meldecodes: Ein neuer Leitstellen-Kanal ist ab Werk auf Zonen-Alarme gestellt, sie gehen als Einbruch E130 auf der Meldelinie der Kamera hinaus. Störungen und Kamera-Sabotage haben eigene Codes. E602 ist allein die Testmeldung, zyklisch oder über „Kanal testen“. Bewegung und KI-Erkennung gehen nie als E602 an die Leitstelle. Im Datenschutzprofil ist die zyklische Testmeldung Pflicht, ohne eingestellten Takt alle 6 Stunden, den Takt stimmen Sie mit der Leitstelle ab. Ein Voralarm E138 für Prüfhinweise ist im Profil aus und nicht freigebbar, Griff-Hinweise gehen nie an die Leitstelle.

Versand: Bei jedem Ereignis kommt die Leitstelle zuerst dran. Quittiert sie nicht innerhalb von 3 Sekunden, gehen die übrigen Kanäle trotzdem raus; ihr Ergebnis steht danach im Meldungsverlauf.

Störmeldungen: Zustände der Griff-Wache (pausiert, zu wenige Bilder, Fehlerhäufung, Skelett-Modell fehlt) gehen nicht an die Leitstelle. Sie stehen im Anlagenwächter und gehen an die übrigen Kanäle.

Verifikationslinks sind 24 Stunden gültig und brauchen einen eigenen Netzweg zur Anlage. Über das Relay sind sie nicht erreichbar. Im Datenschutzprofil gibt es sie nicht. Meldungen tragen keinen Verifikationslink, und die Seite `/verify/` sowie die Bewertung antworten mit dem Hinweis, dass es im Datenschutzprofil für die Bildprüfung nur den Prüflink gibt, auch für schon verschickte Links. Eine früher erteilte Freigabe dafür entfällt beim nächsten Abgleich des Profils (beim Start und stündlich), das steht im Journal. Damit entfällt im Profil auch die Bewertung durch die Leitstelle (Name, Notiz, Ergebnis).

Prüflink: Zu jedem Zonen-Alarm erzeugt die Anlage einen Link auf eine Seite ohne Anmeldung mit dem Ereignisbild, Köpfe der erkannten Personen und Gesichter verpixelt, bei Fahrzeugen der untere Teil, wo in der Regel das Kennzeichen sitzt, ohne Livebild. Er gilt ab Werk 60 Minuten, einstellbar bis höchstens 24 Stunden. Verpixelt werden alle Personen und Fahrzeuge, die die KI im Bild erkennt, auch außerhalb der Zonen und unabhängig von der Objektauswahl der Kamera. Personen zählen dafür schon ab geringer Sicherheit, auch unter der Konfidenz-Schwelle der Kamera. Liegen zum Ereignis keine Erkennungsrahmen vor, zeigt die Seite statt eines Bildes einen kurzen Hinweis. Jeder Aufruf von Seite und Bild steht im Journal (`pruef_ansehen` , `pruef_bild`); gegen das Fluten gilt nur eine Obergrenze von 30 Einträgen je Art und Ereignis in einer Minute, die Zahl der darüber hinaus unterdrückten Aufrufe steht im nächsten Eintrag. Fahrzeuge zählen dafür auch, wenn die KI sie nur unsicher erkennt. Im Datenschutzprofil verpixelt die Anlage bei Auto, Lkw und Bus die unteren 60 Prozent, beim Motorrad das ganze Fahrzeug, und den Kopf nach der Lage der Person (siehe Kapitel Datenschutzprofil, Zeile Prüfbild); ohne gültige Box einer Person oder eines Fahrzeugs zeigt sie dort kein Bild. Den Kopf schätzt LocalEye aus der Lage der Person: Bei ungewöhnlicher Haltung (Kopf unten, frontal gebückt, Kind im Einkaufswagen) kann er sichtbar bleiben, die Prüfseite nennt diese Grenze. Der Webhook trägt ihn als Feld `pruef_link` , im Datenschutzprofil nur mit „Prüflink mitsenden“; ein Webhook mit eigener Vorlage sendet nur die Vorlage, das Feld geht dann nicht hinaus. E-Mail, Push und Teams hängen ihn als Zeile an, wenn am Kanal „Prüflink mitsenden“ an ist, ab Werk ist das aus. Die Leitstelle über SIA DC-09 kann keine Links empfangen, einen festen Weg dorthin stimmen Sie mit ihr ab. Der Meldungsverlauf speichert den Text ohne den Link. Gültigkeit unter Einstellungen, Verbindungen, „Prüflink gültig (Minuten)“, Vorgabe 60, höchstens 1440. Von außen taugt er nur mit gesetzter Öffentlicher Basis-URL.

Clip im Prüflink (ab Werk aus): Mit der Einstellung unter Einstellungen → Verbindungen steht unter dem Prüfbild ein kurzer Clip der 8 Sekunden nach dem Alarm. Die Anlage baut ihn nur, wenn ein Kanal den Prüflink wirklich versendet hat, und holt die Bilder nur über den eigenen Restream der Kamera. Verpixelt sind Köpfe und Gesichter erkannter Personen, bei Fahrzeugen der untere Teil, wo in der Regel das Kennzeichen sitzt, auch bei unsicher erkannten Fahrzeugen. Es gibt keinen Clip, wenn das bei einem einzigen Bild scheitert, wenn die Erkennung die Person oder das Fahrzeug des Alarms in keinem Bild wiederfindet oder wenn der Rechner ausgelastet ist. Eine Person, die Erkennung und Gesichtssuche in einem Bild nicht finden, bleibt dort unverpixelt: Prüfen Sie das an der eigenen Anlage, bevor Sie die Funktion im Betrieb einschalten. Jeder Abruf steht im Journal (`pruef_clip`). Der Clip wird mit seinem Ereignisbild gelöscht und beim Ausschalten sofort, ein gehaltenes Ereignis behält ihn. Er geht in keine Sicherung. Im Datenschutzprofil gibt es ihn nur mit der befristeten Freigabe „Clip im Prüflink“ unter Einstellungen, Funktionen, mit Begründung, Grundlage und Enddatum. Ohne gültige Freigabe steht unter Einstellungen → Verbindungen statt des Schalters ein Hinweis, und die Anlage lehnt das Einschalten ab. Läuft die Freigabe ab oder wird sie entfernt, schaltet der nächste Profillauf den Clip aus und löscht die

fertigen Clips; ein gehaltenes Ereignis behält seinen. Beim Wechsel ins Profil löscht die Anlage Clips, die vorher gebaut wurden. Die Abnahme zeigt „Clip im Prüflink“ als ABWEICHUNG, solange der Clip an ist, auch mit Freigabe.

Prüfzugang der Leitstelle: Die Alarm-Leitstelle prüft einen gemeldeten Zonen-Alarm über ihr VPN direkt auf der Anlage, unter `/leitstelle/`, z. B. `https://<IP>:8943/leitstelle/`. Das gilt mit und ohne Datenschutzprofil. So richten Sie ihn ein:

1. In der `.env` `LEITSTELLE_CIDRS` auf das VPN-Netz der Leitstelle setzen, z. B. `192.168.50.0/24`, mehrere mit Komma. Leer, ein ungültiger Eintrag oder ein Netz über alle Adressen (`0.0.0.0/0`) sperren das Konto ganz. `LEITSTELLE_FENSTER_MIN` legt fest, wie lange ein Alarm ab der Quittung abrufbar ist: Vorgabe 60 Minuten, höchstens 240. `./manage.sh profil edeka` setzt beide Werte nicht.
2. Unter Einstellungen, Benutzer, „+ Benutzer“ ein Konto mit der Rolle „Leitstelle“ anlegen und unter „Gebunden an SIA-Kanäle“ einen oder mehrere SIA-Kanäle wählen. Kanäle ohne Kennung lassen sich nicht binden. Anlegen und Binden gehen nur im lokalen Netz oder per VPN, nicht über den Fernzugriff. Das Passwort setzt der Admin.
3. Beim ersten Anmelden richtet die Leitstelle den zweiten Faktor ein und bekommt Wiederherstellungs-Codes. Bis dahin zeigt die Anlage keinen Alarm und kein Bild. Den zweiten Faktor setzt ein Admin unter Einstellungen, Benutzer zurück.

Die Leitstelle sieht nur Zonen-Alarme (E130), die an einen ihrer SIA-Kanäle gemeldet und dort quittiert wurden, mit Zeit der Quittung, Kamera samt Leitstellen-Nummer und Zone. Dazu kommt das verpixelte Prüfbild mit einem Wasserzeichen aus Konto, Uhrzeit und Anlage. Kein Livebild, keine Aufnahme, kein Clip, kein Download und keine andere Seite der Anlage. Gezeigt werden nur Alarme von Kameras dieser Anlage, nicht die einer Erweiterung im Verbund. Eine Sitzung gilt höchstens 12 Stunden. Über den Fernzugriff, aus einem anderen Netz und solange `LEITSTELLE_CIDRS` leer oder ungültig ist, antwortet `/leitstelle/` wie eine Anlage ohne Leitstellen-Konto mit „nicht gefunden“ (404), nach Ablauf des Zeitfensters mit 410. Passt das Netz einer angemeldeten Leitstelle nicht mehr, endet ihre Sitzung. Ändert ein Admin Ziel, Ersatz-Ziel, Ports oder Kennungen eines gebundenen SIA-Kanals oder löscht ihn, löst die Anlage die Bindung und meldet „Bindung der Leitstelle gelöst, bitte neu zuordnen“. Abweisungen, das Öffnen der Liste, angesehene Ereignisse und Bildabrufe stehen gebündelt im Journal.

18. Störungen beheben

Symptom	Ursache und Abhilfe
Kachel bleibt schwarz	Mit dem Test-Knopf an der Kamera prüfen. H.265 auf H.264 umstellen.
Live bricht im Browser ab	Seite neu laden. Bei eigenem Reverse-Proxy WebSocket erlauben.
Verpasste Erkennungstakte	Unter 2 Prozent unkritisch, sonst Intervall vergrößern oder Kameras verteilen.
Prüfhinweis-Liste bleibt leer	Funktion an? Die Seite und der Wächter zeigen, wenn die Bild-KI nicht antwortet. Ein Hinweis braucht eine erkannte Person und eine verdächtige Handlung im Text. Prüfhinweise sind selten, eine leere Liste ist meist normal.
Keine Meldung kommt an	Kanal aktiviert und gespeichert? Auslöser gewählt und die betroffene Kamera angehakt? „Nur wenn scharf“ gesetzt und Anlage unscharf? Zeitfenster? Cooldown? Verlauf prüfen.
Meldet bei jeder Bewegung	Auslöser Bewegung und KI im Kanal abwählen.
Push kommt unterwegs nicht an	ntfy ist nur erreichbar, wenn der Server von außen erreichbar ist, siehe Kapitel 11.
Fernzugriff offline	TCP 7000 ausgehend, SSL-Inspection, Lizenz, Schalter. Im Datenschutzprofil: Haben alle Admins 2FA?
Im Fernzugriff abgemeldet	Portal-Sitzung nach 12 Stunden abgelaufen. Neu anmelden.
2FA-Code wird abgelehnt	Uhr von Handy und Anlage prüfen. Bei „Dieser Code wurde schon verwendet. Bitte den nächsten Code abwarten.“ den nächsten Code der App nehmen.
Anmeldung gesperrt	Nach fünf Fehlversuchen kurz warten.
Passwort vergessen	Ein anderer Admin setzt es zurück.
Update bricht ab	Log prüfen, Internetzugang zu den Quellen prüfen. Release-Datei erneut hochladen, „Vollständig neu bauen (--no-cache)“ anhaken.
Update wird abgelehnt	Paket verändert, unsigniert oder älter als die installierte Version.
Speicher-Warnung	Fristen prüfen, Platz schaffen, Speicher erweitern. Aufnahmen und Snapshots löscht die Anlage ohne Frist nicht.
Neuer Schlüssel abgelehnt	Der bisherige bleibt aktiv, die Dienste laufen weiter. Schlüssel prüfen.
Alle Dienste nach einem Neustart gestoppt	Der Lizenzserver hat den Schlüssel abgelehnt. In der Shell `./manage.sh activate <Schlüssel>` mit dem richtigen Schlüssel ausführen.
Verbund-Standort rot	Netzweg und Gerät prüfen, Uhren prüfen. Nach Rückkehr heilt es selbst.
Kein Lizenz-Slot	Erweiterungs-Token einlösen oder Standort trennen, 14 Tage Karenz.
KI meldet „Modell nicht geladen“	`./manage.sh logs` lesen.

Symptom	Ursache und Abhilfe
„Verwaltung im Datenschutzprofil nur lokal im Markt erreichbar“	Im Profil sind Verwaltungsfunktionen über den Fernzugriff gesperrt. Im Markt-LAN oder per VPN anmelden.
„… nur aus dem festgelegten Markt-LAN erreichbar“	Die Adresse liegt nicht in `VERWALTUNG_LAN_CIDRS`. Vom freigegebenen Netz aus arbeiten oder den Bereich in der `.env` anpassen. Am Gerät geht die Verwaltung immer.
„Kein Adressbereich für die Verwaltung festgelegt. Bitte VERWALTUNG_LAN_CIDRS eintragen.“	Im Datenschutzprofil ist kein Markt-LAN eingetragen, die Verwaltung geht nur am Gerät. Am Bildschirm der Anlage arbeiten oder den Bereich eintragen: `./manage.sh profil edeka` am Terminal, in der `.env` oder am Gerät in „Anlage verwalten“, Karte Datenschutzprofil.
„Adressbereich für die Verwaltung ungültig. …“	`VERWALTUNG_LAN_CIDRS` prüfen: Netze wie `192.168.1.0/24`, mehrere mit Komma, kein Bereich über alle Adressen. Bis dahin nur am Gerät verwaltbar.
„Verwaltung dieser Erweiterung über die Hauptanlage gesperrt …“	Die Hauptanlage prüft den Zugriff nicht selbst (ohne Datenschutzprofil oder ältere Fassung). Hauptanlage aktualisieren und ins Profil nehmen, bis dahin der Notzugang der Erweiterung: `./manage.sh notfall-gui an`.
„Im Datenschutzprofil gibt es Kamerabilder nur nach Anmeldung.“ (410)	Gewollt. Im Profil liefern API-, Schnappschuss- und Leitstand-Token keine Bilder, eine Freigabe dafür gibt es nicht.
Sicherung oder Zurückspielen bricht im Datenschutzprofil ab	Kein gültiges Sicherungs-Passwort oder openssl fehlt. `sudo ./manage.sh sicherung-passwort` oder Karte Sichern, openssl ab Version 1.1.1 installieren.
Clip im Prüflink lässt sich nicht einschalten	Im Datenschutzprofil nur mit gültiger, befristeter Freigabe „Clip im Prüflink“.
Leitstelle sieht „nicht gefunden“	`LEITSTELLE_CIDRS` leer, ungültig oder ohne das Netz der Leitstelle, Zugriff über den Fernzugriff oder kein Konto mit der Rolle Leitstelle. „Nicht mehr abrufbar“ (410) heißt: Zeitfenster ab der Quittung abgelaufen.
Oberfläche aus dem Netz nicht erreichbar	Bei `LAN_HTTP=aus` `https://<IP>:8943/` verwenden, HTTP leitet nur noch dorthin um. Ohne eingerichtetes HTTPS geht es dann nur am Gerät.
Leitstelle bekommt keine Bewegungsmeldungen mehr	Gewollt. Bewegung und KI-Erkennung gehen nicht an die Leitstelle, Zonen-Alarme als E130.
Prüfhinweis-Liste ohne Beschreibung	Im Datenschutzprofil ist die Bildbeschreibung bis zur Freigabe aus.

Hersteller kontaktieren: Halten Sie Version, Ausgabe von `./manage.sh selbsttest` und den Statusbericht aus „Anlage verwalten“ bereit. Geben Sie keine Passwörter, Lizenzschlüssel oder Wiederherstellungs-Codes weiter.

19. Referenz

Befehle

Alle Befehle im Installationsordner ausführen. Die Weboberfläche ruft dieselben Befehle auf, die Shell ist der Rückfall.

Befehl	Zweck
`./manage.sh update <zip>`	Installieren oder aktualisieren
`./manage.sh update-pruefen`	Im Shop nach einer neueren Version sehen
`./manage.sh update-online`	Neue Version aus dem Shop einspielen
`./manage.sh start`, `stop`, `restart`	Dienste steuern. Stopp beendet auch Aufnahmen und Alarme.
`./manage.sh status`, `logs`	Zustand und Protokolle
`./manage.sh selbsttest`	Vollständige Prüfung
`./manage.sh activate <Schlüssel>`	Lizenz aktivieren oder wechseln. Ein abgelehnter Schlüssel ändert nichts.
`./manage.sh config`	Verwaltung starten, Adresse und neuen Einrichtungscode anzeigen
`./manage.sh 2fa-zuruecksetzen <Benutzer>`	2FA eines Kontos zurücksetzen, wenn Handy und Codes weg sind
`./manage.sh backup`, `restore`	Sicherung in der Shell, braucht root. `restore ziel:<datei>` spielt eine Sicherung vom Sicherungsziel ein, `restore ziel:` zeigt die Sicherungen dort.
`./manage.sh sicherung-passwort [entfernen]`	Sicherungs-Passwort setzen, ändern oder entfernen. Ein neues Passwort gilt für neue Sicherungen; ältere brauchen ihr bisheriges. Im Datenschutzprofil entsteht ohne Passwort keine Sicherung.
`./manage.sh sicherung-frist`	Im Datenschutzprofil eigene Sicherungen löschen, die älter als `SICHERUNG_FRIST_TAGE` sind (leer 7 Tage), mit Eintrag im Journal. Das tun auch jede neue Sicherung und der tägliche Fristlauf. Braucht root.

Befehl	Zweck
`./manage.sh ki-sandbox`, `absichern`, `zurueck`	`./manage.sh ki-sandbox` zeigt, wie die Docker-Sandbox der KI läuft. `./manage.sh ki-sandbox absichern` stellt sie auf einen Docker-Daemon ohne Root um: Eine KI-Sitzung kann dann über die Sandbox nicht mehr Root auf dem Gerät werden. Images, Container und Volumes, die KI-Sitzungen bisher in der Sandbox angelegt haben, bleiben im alten Speicher; `./manage.sh ki-sandbox zurueck` holt sie zurück. Neue Installationen wählen die abgesicherte Art beim ersten Start selbst, wenn das Gerät sie unterstützt. Die Offline-ISO bringt die KI-Sandbox in beiden Arten mit. Beim ersten Start erprobt die Anlage die abgesicherte Art ohne Internet und wählt sie, wenn das Gerät sie unterstützt. `./manage.sh ki-sandbox absichern` und `zurueck` brauchen auf einer solchen Anlage kein Internet. Der Docker-Daemon der KI-Sandbox ist nur über den Socket erreichbar, den KnowSora nutzt, nicht über das Netz. Der Selbsttest prüft das.
`./manage.sh port list`	Ports anzeigen
`./manage.sh webgui`	Oberfläche im Terminal
`./manage.sh gpu status`	GPU-Stand
`./manage.sh join`	Erweiterung koppeln
`./manage.sh notfall-gui an`, `aus`	Notzugang einer Erweiterung
`./manage.sh kopplungscode`	Einmalcode einer Erweiterung für die Einladung durch die Hauptanlage
`./manage.sh profil <name> [--ja]`	Voreinstellung aus `.env.<name>.example` übernehmen, etwa `edeka`. Fragt nach, `--ja` übernimmt ohne Rückfrage. Ist `VERWALTUNG_LAN_CIDRS` leer oder ungültig, fragt er am Terminal danach.
`./manage.sh abnahme`	Abnahmeprotokoll Datenschutzprofil: jede Vorgabe mit OK/ABWEICHUNG/NICHT PRÜFBAR, Ablage unter logs/, Exit 1 bei Abweichungen. Mit `sudo` aufrufen, damit er auch die Sicherungen prüft.

Ablage

Pfad	Inhalt
`localeye/config/`	Kameras, Zonen, Benutzer, Einstellungen, Geheimnisse
`localeye/recordings/`	Aufnahmen
`localeye/snapshots/`	Snapshots
`localeye/ai_reports/`	KI-Berichte
`backups/`	Lokale Sicherungen
`.env`	Ports, Betriebsart, Profile, Lizenz

> `.env` und `localeye/config/` enthalten Geheimnisse. Geben Sie sie nicht weiter.

Zeiten und Fristen

Was	Wert
Lizenzprüfung	alle 24 Stunden
Portal-Sitzung	12 Stunden
LocalEye-Sitzung	30 Tage ab letzter Nutzung
Aufbewahrung im Datenschutzprofil	höchstens 72 Stunden, siehe Kapitel 7
Audit-Journal	Vorgabe 365 Tage
Verifikationslink	24 Stunden, im Datenschutzprofil keiner
Prüflink	Vorgabe 60 Minuten, höchstens 24 Stunden
Clip im Prüflink	wie das Ereignisbild, beim Ausschalten sofort gelöscht; im Datenschutzprofil nur mit befristeter Freigabe, nach deren Ablauf gelöscht
Prüfzugang der Leitstelle	Vorgabe 60 Minuten ab der Quittung (`LEITSTELLE_FENSTER_MIN`), höchstens 240; Sitzung höchstens 12 Stunden
Sicherungen im Datenschutzprofil	`SICHERUNG_FRIST_TAGE` , leer 7 Tage; Fristlauf täglich
Gedächtnis der Griff-Wache für getragene Ware	bis zu 60 Sekunden, nur im Arbeitsspeicher
Manuelle Aufnahme im Datenschutzprofil	höchstens 2 Stunden
Zyklische Testmeldung im Datenschutzprofil	ohne eingestellten Takt alle 6 Stunden
Entscheidungen zu Prüfhinweisen, gelernte Fehlalarm-Muster und Rückmeldungen im Lernlauf-Bericht im Datenschutzprofil	72 Stunden
Karenz Verbund-Slot	14 Tage
Wächter	jede Minute, Störung nach drei Treffern