Administratoren-Handbuch

Konfiguration und Verwaltung

EINFO – Einsatzinformationssystem

Benutzerhandbuch

1. Übersicht

Das Admin-Panel ist die zentrale Verwaltungsoberfläche von EINFO. Es ist ausschließlich für Benutzer mit der Rolle „Admin“ zugänglich und erreichbar unter /user-admin.

Im Admin-Panel können Sie folgende Bereiche konfigurieren:

- Master-Key Verwaltung (Erststart und Entsperrung)
- Rollen und Berechtigungen für alle drei Boards
- Benutzerverwaltung (Anlegen, Bearbeiten, Löschen)
- Import-Einstellungen (Auto-Import und Demomodus)
- Auto-Druck für Protokolleinträge
- KI-Analyse (Situationsanalyse mit optionalem RAG-Kontext)
- Zeitgesteuerter Mailversand
- Zeitgesteuerte API-Calls
- Fetcher-Zugangsdaten
- Chatbot & Worker-Steuerung
- Knowledge-Basis (RAG) für den Chatbot
- Hybrid-Filtersystem (Regeln R1–R5)
- KI-Modell-Verwaltung (Ollama)

2. Wichtige URLs

Die folgenden Seiten sind über den Browser erreichbar (Standard-Port: 4040):

- / – Einsatzboard (Hauptansicht)
- /aufgaben – Aufgabenboard
- /status – Statusseite (druckfreundlich mit ?print=1)
- /user-login – Login-Seite
- /user-admin – Admin-Panel
- /user-firststart – Erststart-Assistent
- /Hilfe.pdf – Benutzerhandbuch Einsatzboard
- /Hilfe_Aufgabenboard.pdf – Benutzerhandbuch Aufgabenboard
- /Hilfe_Meldestelle.pdf – Benutzerhandbuch Meldestelle

3. Erststart & Master-Key

3.1 Erststart

Beim allerersten Start der Anwendung muss der Master-Key gesetzt und ein erster Admin-Benutzer angelegt werden. Navigieren Sie dazu zu /user-firststart.

- Master-Key – Wählen Sie ein sicheres Passwort als Master-Key.
- Admin-Benutzer – Benutzername und Passwort für den ersten Administrator.

Der Master-Key wird benötigt, um nach jedem Server-Neustart das System zu entsperren.

3.2 Master entsperren (nach Neustart)

Nach einem Server-Neustart ist das System gesperrt (423 Master-Lock). Navigieren Sie zum Admin-Panel (/user-admin) und geben Sie den Master-Key im Bereich „Master entsperren“ ein. Erst danach können Benutzer und Rollen verwaltet werden.

3.3 Board zurücksetzen

Im Admin-Panel steht oben rechts die Schaltfläche „Reset“ zur Verfügung. Damit wird das Einsatzboard komplett zurückgesetzt. Es erscheint eine Sicherheitsabfrage. Verwenden Sie diese Funktion nur im Notfall oder für Testszenarien.

4. Rollen und Berechtigungen

4.1 Rollenkonzept

Jede Rolle definiert die Zugriffsrechte auf die drei Boards: Einsatzboard, Aufgabenboard und Protokoll (Meldestelle). Pro Board gibt es drei Berechtigungsstufen:

- none – Kein Zugriff auf dieses Board.
- view – Nur-Ansicht. Der Benutzer kann Daten sehen, aber nicht ändern.
- edit – Vollzugriff. Der Benutzer kann anlegen, bearbeiten und löschen.

Die Rolle „Admin“ hat immer „edit“ auf allen Boards und kann nicht gelöscht oder eingeschränkt werden.

4.2 Standard-Rollen

Rolle	Beschreibung	Berechtigung
Admin	Systemadministrator	edit auf allen Boards
LtStb	Leiter Stab	edit auf allen Boards
S1	Personal	view/edit je nach Config
S2	Lage und Information	edit auf allen Boards
S3	Einsatz / Operation	view/edit je nach Config
S4	Versorgung / Logistik	view/edit je nach Config
S5	Öffentlichkeitsarbeit	view/edit je nach Config
S6	IT / Kommunikation	view/edit je nach Config
MS	Meldestelle	edit auf Protokoll
Mitarbeiter	Allgemeiner Mitarbeiter	view

4.3 Rollen verwalten

Im Bereich „Rollen (Admin + weitere)“ können Sie:

- Neue Rollen hinzufügen: Name eingeben und „Hinzufügen“ klicken.
- Rollen entfernen: Auf das × neben dem Rollennamen klicken.
- Rechte pro Rolle: In der Tabelle „Rechte pro Rolle“ die Berechtigungsstufe (none/view/edit) für jedes Board per Dropdown einstellen.
- Mit „Rollen speichern“ bzw. „Rechte speichern“ die Änderungen sichern.

5. Benutzerverwaltung

5.1 Benutzer anlegen

Geben Sie im Formular folgende Felder ein:

- Username – Eindeutiger Benutzername zum Einloggen.
- Passwort – Initiales Passwort für den Benutzer.
- Anzeigename – Wird in der Oberfläche angezeigt.
- Rollen – Wählen Sie eine oder mehrere Rollen aus der Liste. Mehrfachauswahl über Strg (Windows) oder ⌘ (macOS).

5.2 Benutzer bearbeiten

Klicken Sie auf „Edit“ neben einem Benutzer, um Anzeigename, Rollen oder Passwort zu ändern. Das Passwort wird nur aktualisiert, wenn ein neues eingegeben wird. Speichern Sie mit „Save“ oder brechen Sie mit „Cancel“ ab.

5.3 Benutzer löschen

Klicken Sie auf „Del“ neben einem Benutzer. Es erscheint eine Sicherheitsabfrage. Gelöschte Benutzer können nicht wiederhergestellt werden.

6. Relevante Speicherorte

Alle persistenten Daten liegen unter server/data/:

- Aufg_board_<ROLLE>.json – Board-Daten pro Rolle (z. B. Aufg_board_S2.json)
- Aufg_log.csv – Globales Aufgaben-Log
- Aufg_log_<ROLLE>.csv – Rollenbezogene Logs
- User_roles.json – Rollendefinitionen und Berechtigungen
- User_users.enc.json – Verschlüsselte Benutzerdaten
- User_authIndex.json – Login-Index
- User_master.json – Master-Key Information
- protocol.json / protocol.csv – Protokolldaten
- prints/protokoll_*.pdf – Gedruckte Protokolle
- conf/filtering_rules.json – Filterregel-Definitionen (R1–R5)
- conf/ai-analysis.json – KI-Analyse-Konfiguration
- llm_feedback/learned_filters.json – Gelernte Filtergewichte
- scenario_config.json – Szenario-Konfiguration

Der Frontend-Build (inkl. Hilfe-PDFs) liegt unter server/dist/.

7. Import-Einstellungen

7.1 Auto-Import

Der Auto-Import ruft in konfigurierbaren Intervallen externe Einsatzdaten ab. Im Admin-Panel können Sie folgende Parameter einstellen:

- Aktiviert/Deaktiviert – Schaltet den automatischen Import ein oder aus.
- Intervall (Sekunden) – Abstand zwischen zwei Import-Zyklen. Minimum: 5 Sekunden, Maximum: 3600 Sekunden (1 Stunde).
- Demomodus – Wenn aktiviert, wird der Fetcher beim Import nicht gestartet. Nützlich für Tests oder Präsentationen mit statischen Daten.

7.2 Fetcher-Zugangsdaten

Im Bereich „Fetcher-Zugangsdaten (global)“ können die Zugangsdaten für externe Datenquellen hinterlegt werden. Diese werden vom Import-Modul verwendet, um Einsatzdaten abzurufen.

8. Auto-Druck (Protokoll)

Der Auto-Druck generiert in regelmäßigen Abständen automatisch PDF-Ausdrucke der Protokolleinträge. Die Konfiguration umfasst:

- Aktiviert/Deaktiviert – Schaltet den automatischen Druck ein oder aus.
- Intervall (Minuten) – Zeitabstand zwischen zwei Druckläufen. Minimum: 1 Minute.
- Umfang (Scope) – Bestimmt, welche Einträge gedruckt werden:
  - „Intervall“ – Nur Einträge seit dem letzten Drucklauf.
  - „Alle“ – Alle vorhandenen Protokolleinträge.

Der Zeitpunkt des letzten Drucklaufs wird im Admin-Panel angezeigt. Gedruckte PDFs werden unter server/data/prints/ abgelegt.

9. KI-Analyse (Situationsanalyse)

Die KI-Analyse erstellt in regelmäßigen Abständen eine automatische Situationseinschätzung auf Basis der aktuellen Einsatz- und Protokolldaten.

- Aktiviert/Deaktiviert – Schaltet die automatische Analyse ein oder aus.
- Intervall (Minuten) – Zeitabstand zwischen zwei Analyseläufen. Wert 0 bedeutet: nur manuelle Auslösung.
- RAG-Kontext verwenden – Wenn aktiviert, werden zusätzlich Informationen aus der Knowledge-Basis (Wissensdatenbank) in die Analyse einbezogen. Dies kann die Qualität der Einschätzung verbessern, erhöht aber die Verarbeitungszeit.

10. Zeitgesteuerter Mailversand

Im Bereich „Zeitgesteuerter Mailversand“ können Sie wiederkehrende E-Mail-Versandaufträge konfigurieren. Jeder Zeitplan hat folgende Felder:

- Bezeichnung – Interner Name für den Zeitplan.
- Empfänger (An) – E-Mail-Adresse(n) der Empfänger.
- Betreff – Betreffzeile der E-Mail.
- Text – Nachrichteninhalt.
- Anhang-Pfad – Optionaler Dateipfad für einen Anhang.
- Modus – „Intervall“ (alle X Minuten) oder „Feste Uhrzeit“ (täglich zu einer bestimmten Uhrzeit).
- Aktiviert – Ob der Zeitplan aktiv ist.

Bestehende Zeitpläne können bearbeitet, gelöscht oder der letzte Versandzeitpunkt zurückgesetzt werden.

11. Zeitgesteuerte API-Calls

Im Bereich „Zeitgesteuerte API-Calls“ können automatische HTTP-Anfragen an externe Systeme konfiguriert werden. Jeder Zeitplan umfasst:

- Bezeichnung – Interner Name für den Zeitplan.
- URL – Ziel-URL für den HTTP-Aufruf.
- Methode – HTTP-Methode (GET, POST, PUT, DELETE).
- Body – Optionaler Request-Body (für POST/PUT).
- Modus – „Intervall“ (alle X Minuten) oder „Feste Uhrzeit“ (täglich).
- Aktiviert – Ob der Zeitplan aktiv ist.

Zeitpläne können bearbeitet, gelöscht oder der letzte Aufrufzeitpunkt zurückgesetzt werden.

12. Chatbot & Worker

12.1 Chatbot-Steuerung

Der EINFO-Chatbot basiert auf einem lokalen LLM (Llama 3.1) und nutzt RAG (Retrieval-Augmented Generation) für kontextbezogene Antworten. Im Admin-Panel können Sie den Chatbot starten und stoppen. Der aktuelle Status (Running/Stopped) wird automatisch alle 5 Sekunden aktualisiert.

12.2 Worker-Steuerung

Der Worker ist ein Hintergrundprozess, der regelmäßig Aufgaben wie Datenaufbereitung, Analyse und Synchronisation durchführt. Sie können den Worker starten und stoppen.

12.3 Worker-Intervall

Im Bereich „Worker-Intervall Einstellung“ legen Sie fest, wie oft der Worker seine Aufgaben ausführt. Das Intervall wird in Sekunden angegeben (Minimum: 5 Sekunden). Zusätzlich kann der Worker hier aktiviert oder deaktiviert werden.

13. Knowledge-Basis (RAG)

Die Knowledge-Basis enthält Dokumente, die der Chatbot als Wissensquelle nutzt. Neue Dateien (PDF, JSON, TXT) können hochgeladen werden.

- Dateien hochladen – Wählen Sie eine oder mehrere Dateien über den Upload-Button aus.
- Dateien anzeigen – Die Liste zeigt alle vorhandenen Dateien in der Knowledge-Basis mit Dateiname und Größe.
- Dateien löschen – Einzelne Dateien können aus der Knowledge-Basis entfernt werden.
- Ingest starten – Nach dem Hochladen neuer Dateien muss ein Ingest (Indizierung) gestartet werden, damit die Inhalte im RAG-System verfügbar werden. Dieser Vorgang kann einige Minuten dauern.

14. Hybrid-Filtersystem (R1–R5)

Das Filtersystem besteht aus fünf konfigurierbaren Regeln, die steuern, welche Daten dem Chatbot als Kontext bereitgestellt werden. Die Regeln können einzeln aktiviert oder deaktiviert werden.

R1 – Abschnitte-Priorität

Filtert Abschnitte nach Priorität und zeigt die wichtigsten. Berücksichtigt kritische Einsätze, Gesamtzahl der Einsätze, Personalstärke und durchschnittlichen Personaleinsatz pro Einsatz.

R2 – Protokoll-Relevanz

Filtert Protokoll-Einträge nach Relevanz. Bewertet Einträge anhand konfigurierbarer Faktoren wie offene Fragen, Ressourcen-Anfragen, Statusmeldungen, Dringlichkeit und Warnungen. Einige Faktoren sind „lernbar“ und passen ihre Gewichtung automatisch an.

R3 – Trend-Erkennung

Erkennt Trends in der Einsatzentwicklung über konfigurierbare Zeitfenster (Standard: 60 und 120 Minuten). Erstellt Prognosen für den zukünftigen Einsatzverlauf.

R4 – Ressourcen-Status

Analysiert den Ressourcen-Status und erkennt Engpässe. Hebt Bereiche mit hoher Auslastung hervor (Standard-Schwelle: 80%).

R5 – Stabs-Fokus

Aggregiert Daten für die Stabs-Ansicht. Zeigt nur kritische Einzeleinsätze (z. B. Personen in Gefahr, Evakuierungen, kritische Infrastruktur). Die Scoring-Faktoren und Schwellenwerte sind im Admin-Panel konfigurierbar.

Gelernte Filter

Das System lernt aus Benutzer-Feedback automatisch, welche Filterkriterien hilfreich waren. Die gelernten Gewichte können im Admin-Panel eingesehen und bei Bedarf zurückgesetzt werden.

15. KI-Modell-Verwaltung

Im Bereich „KI-Modell-Verwaltung“ werden die lokal verfügbaren LLM-Modelle (via Ollama) verwaltet. Sie können:

- Verfügbare Modelle auflisten und deren Status einsehen.
- Neue Modelle herunterladen (Pull).
- Das aktive Modell für den Chatbot und die Analyse auswählen.

16. Konfiguration (.env)

Folgende Umgebungsvariablen können in der .env-Datei gesetzt werden:

- PORT – Server-Port (Standard: 4040).
- FF_AUTO_STOP_MIN – Automatische Abschaltzeit in Minuten (Standard: 60). Nach dieser Inaktivitätszeit wird der Fetcher gestoppt.

17. Backup & Recovery

Erstellen Sie regelmäßig Backups des Verzeichnisses server/data/ vor größeren Änderungen. Das Verzeichnis enthält alle persistenten Daten:

- Benutzer- und Rollendaten
- Einsatz- und Aufgabenboards
- Protokolldaten und gedruckte PDFs
- Filterregeln und gelernte Gewichte
- Szenario- und Analyse-Konfigurationen

Bei verlorenem Admin-Zugang

Sichern Sie die Dateien User_master.json und User_users.enc.json. Entfernen Sie diese Dateien und starten Sie den Server neu. Navigieren Sie zu /user-firststart, um einen neuen Master-Key und Admin-Benutzer anzulegen. Die Rollendefinitionen (User_roles.json) bleiben dabei erhalten.

Wartung

Im Admin-Panel steht im Bereich „Wartung (Admin)“ eine Funktion zum Herunterladen von Backup-Dateien und Logdateien zur Verfügung. Nutzen Sie diese regelmäßig, um Datenverluste zu vermeiden.