FF Operation

Anleitung

bis v1.3.x

Open Source Software
entwickelt durch JK Effects
von Julian Krauser

15. März 2026

Inhaltsverzeichnis

1 Einleitung

FF Operation - Flexibles Einsatz- und Übungsmanagement für Feuerwehren und Vereine

FF Operation ist eine leistungsfähige Verwaltungssoftware und ein zentraler Bestandteil des FF-Ökosystems. Neben Feuerwehreinsätzen oder Übungen können auch Arbeitseinsätze von Vereinen erfasst werden. Durch den modularen Aufbau und frei definierbare Stammdaten kann die Software flexibel an unterschiedliche Organisationen angepasst werden.

FF Operation ermöglicht darüber hinaus die kollaborative Erstellung von Einsatzberichten, sowie die Synchronisierung von Daten, wenn ein Gerät zwischenzeitlich offline war.

Wird FF Admin eingesetzt, kann es als zentrale Datenquelle für Basisinformationen der Anwendung dienen.

2 Installation

FF Operation kann über mehrere Wege betrieben werden. Zum einen werden Docker-Images versioniert zur Verfügung gestellt. Weiterhin kann auch das Release Projekt heruntergeladen und verwendet werden.

2.1 Docker

Disclaimer: Die Anleitung zum Betrieb von FF Operation mit Docker setzt Kenntnisse mit Docker und Docker-Compose voraus.

Die Docker-Images können gemeinsam über eine Compose-File konfiguriert und gestartet werden. Auch können die Images einzeln gestartet werden.

Die Docker-Images sind versioniert. Der `<tag>` des Images kann entweder `latest` für die neueste Version oder `vX.Y.Z` für eine bestimmte Version sein. Die Versionen können auch in den Releases der Repositories der Anwendungen nachgeschlagen werden. Dort lassen sich auch auch Informationen zu neuen Funktionen, Änderungen oder Fehlerbehebungen der jeweiligen Funktion finden.

2.2 Docker-Compose

App

```yaml
ff-operation-app:
  image: code.jk-effects.cloud/ff-admin/ff-operation/app:<version | latest>
  container_name: ff_operation
  restart: unless-stopped
  ports:
    - "80:80"
  environment:
    - SERVERADDRESS=<backend_url> # optional, bei abweichender URL des Backends
```

Die Verwendung der Werte des Typs Environment werden unter dem Punkt Konfiguration (Abschnitt 2.4) erklärt.
Die Environment-Variable `SERVERADDRESS` ist optional und kann für eine Abweichende URL des Backends verwendet werden. Ist die Serveradresse nicht angegeben, wird versucht das Backend unter der selben URL mit dem PathPrefix `/api` zu erreichen.

Eine erweiterte Personalisierung der App mit eigenem Logo der Feuerwehr oder des Vereins ist bei der ersten Einrichtung oder unter dem Modul Einstellungen möglich. Hiervon betroffen ist das Icon im Browser-Tab, jede Anzeige des FF Operation Logos innerhalb der App und das Icon, wenn die WebApp auf einem Gerät installiert wird.

Server

```yaml
ff-operation-server:
  image: code.jk-effects.cloud/ff-admin/ff-operation/server:<version | latest>
  container_name: ff_operation_server
  restart: unless-stopped
  ports:
    - "5000:5000"
  environment:
    - DB_HOST=<database host>
    - DB_PORT=<database port> # optional, da default 5432
    - DB_NAME=<database name>
    - DB_USERNAME=<database username>
    - DB_PASSWORD=<database password>
    - APPLICATION_SECRET=<jwt secret>
    # \/ optional \/
    - USE_SECURITY_STRICT_LIMIT=<boolean>
    - SECURITY_STRICT_LIMIT_WINDOW=<time window>
    - SECURITY_STRICT_LIMIT_REQUEST_COUNT=<strict_request_count>
    - USE_SECURITY_LIMIT=<boolean>
    - SECURITY_LIMIT_WINDOW=<time window>
    - SECURITY_LIMIT_REQUEST_COUNT=<request_count>
    - TRUST_PROXY=<proxy config>
  volumes:
    - <volume|local path>:/app/files
```

Die Verwendung der Werte des Typs Environment werden unter dem Punkt Konfiguration (Abschnitt 2.4) erklärt.
Environment Werte können optional sein oder haben Standard-Werte.
Das Fehlen einer geforderten Variable oder die falsche Angabe eines Variablen-Werts verhindert das Starten des der Anwendung.

Innerhalb dem Ordner, der dem Volume zugeordnet ist, werden Backups und Ausdrucke der geschriebenen Protokolle, Newsletter und alle weiteren Dokumente abgelegt, die hochgeladen oder erstellt werden können.

Datenbank

Als Datenbank wird Postgres verwendet:

```yaml
ff-db:
  image: postgres:<version (bsp 16)>
  container_name: ff_db
  restart: unless-stopped
  ports:
    - "5432:5432"
  environment:
    - POSTGRES_DB=<database name>
    - POSTGRES_USER=<username>
    - POSTGRES_PASSWORD=<user password>
  volumes:
    - <volume|local path>:/var/lib/postgresql/data
```

`POSTGRES_DB` erstellt direkt eine Datenbank, die durch einen angelegten `POSTGRES_USER` verfügbar ist.

Hinweis Wenn eine Docker-Compose Datei verwendet wird, kann zusätzliche ein Netzwerk angelegt werden. Dadurch ist das Veröffentlichen der Datenbank-Ports nicht mehr notwendig. Das Entfernern der Port-Exposes verhindert den direkten Zugriff auf die Ports von außerhalb.
Hierfür muss das verwendete `network` dem Backend und dem Datenbank-Container bekanntgegeben werden:

1. Ergänzung zu Server und Datenbank Container:

```yaml
#volumes:
#  ...
networks:
  - ff_internal
```

2. Ergänzung zur Docker-Compose:

```yaml
networks:
  ff_internal:
```

3. Neue Host-URL der Datenbank des Servercontainers:

```yaml
environment:
  - DB_HOST: ff-db
  # ...
```

Wenn die Datenbank über ein Netzwerk in einer Compose-Datei freigegeben wird, kann als Host der Service-Name der Datenbank angegeben werden. In der angegebenen Datenbank-Konfiguration wäre das `ff-db`.

Optionale Ergänzung zum Servercontainer:

```yaml
#volumes:
#  ...
#networks:
#  - ff_internal
depends_on:
  - ff-db
```

Hierdurch kann der Server nicht starten, wenn die verwendete Datenbank nicht läuft.

Proxy

Damit die App und der Server aus dem Internet über URLs erreichbar sind, kann Traefik oder Nginx als Reverse-Proxy verwendet werden.
Bei der Konfiguration des Proxies ist Folgendes zu beachten:

- Die Tatsächliche IP sollte an den Server weitergeleitet werden
- Alle HTTP-Header müssen an den Server weitergeleitet werden
- Die maximale Größe für Dateiuploads sollte nicht zu stark eingeschränkt werden

Die Weiterleitung der Header kann im Serverlog überprüft werden. API-Anfragen werden im Format `:remote-addr :method :url :status - :response-time ms | isPWA: :headers["x-pwa-client"] - device: :headers["x-device-name"]` protokolliert. Fehlen die Werte nach „isPWA:“ oder „device:“, werden die entsprechenden Header nicht weitergeleitet.

Hinweis: Bei Anfragen von externen APIs oder beim Zugriff auf Logo bzw. Favicon existieren keine benutzerdefinierten Header, da diese nur von der WebApp über den Browser gesendet werden.

2.3 Git

Eine Alternative zu Docker ist die direkte Ausführung der Anwendungen auf dem Server oder einem Desktop Gerät.
Hierzu müssen die App und der Server als Quellcode auf das ausführende System geladen und dort direkt verwendet werden. Das System muss NodeJs 24 und Postgres installiert haben.

Für das Hosting von statischen Inhalten wie der App kann Apache oder Nginx verwendet werden. Eine Konfiguration für Nginx ist im Repo der App enthalten:

```conf
worker_processes 4;

events { worker_connections 1024; }

http {
  include mime.types;

  server {
    root /usr/share/nginx/html; # Pfad zum dist Ordner des Frontends
    index index.html;

    location / {
      try_files $uri $uri/ /index.html;
    }
  }
}
```

Die NodeJs Prozesse können auch durch Tools wie pm2 verwaltet werden.
Damit die App und der Server aus dem Internet erreichbar sind, muss das Routing gesondert eingerichtet werden.

Um die Konfiguration mittels ENV-Variablen an die Anwendungen weitergeben zu können, müssen `.env` Dateien erstellt werden. Hierzu kann die `.env.example` Datei kopiert und die definierten Werte ausgefüllt werden. Nicht benötigte Einträge sollten entfernt werden.
Die env-Datei im Frontend muss vor dem build-Prozess erstellt sein, da dort die Werte fest in den Code übernommen werden. Weiterhin muss die Datei im Frontend `.env.production` heißen. Die bestehende Datei kann modifiziert werden. Bei einer Änderung muss die App neu gebaut werden. Wird der Server unter der gleichen URL wie die App verwendet, muss in der `.env.production` Datei des Frontends der Wert zum Eintrag von `SERVERADDRESS` auf den leeren String gesetzt werden.

Die env-Datei im Backend muss vor der Ausführung von `npm run start` angelegt sein. Bei einer Änderung der Einträge muss der Server lediglich neu gestartet werden.

App

```Shell
git clone https://code.jk-effects.cloud/ff-admin/ff-operation.git
cd ff-operation
npm install
npm run build
```

Der mit `npm run build` erstellte dist Ordner kann mit Apache oder Nginx zur veröffentlicht werden.

Server

```Shell
git clone https://code.jk-effects.cloud/ff-admin/ff-operation-server.git
cd ff-operation-server
npm install
npm run build
npm run start
```

Proxy

Damit die App und der Server aus dem Internet über URLs erreichbar sind, kann Traefik oder Nginx als Reverse-Proxy verwendet werden.
Bei der Konfiguration des Proxies ist Folgendes zu beachten:

- Die Tatsächliche IP sollte an den Server weitergeleitet werden
- Alle HTTP-Header müssen an den Server weitergeleitet werden
- Die maximale Größe für Dateiuploads sollte nicht zu stark eingeschränkt werden

Die Weiterleitung der Header kann im Serverlog überprüft werden. API-Anfragen werden im Format `:remote-addr :method :url :status - :response-time ms | isPWA: :headers["x-pwa-client"] - device: :headers["x-device-name"]` protokolliert. Fehlen die Werte nach „isPWA:“ oder „device:“, werden die entsprechenden Header nicht weitergeleitet.

Hinweis: Bei Anfragen von externen APIs oder beim Zugriff auf Logo bzw. Favicon existieren keine benutzerdefinierten Header, da diese nur von der WebApp über den Browser gesendet werden.

2.4 Konfiguration

Folgende Werte können zu einem Container konfiguriert werden:

Variable	Zweck	Default	Optional
⬇️ App-Variablen			
SERVERADDRESS	URL, über welche das Backend erreicht werden kann. Die URL muss mit http:// oder https:// starten. Jeder angegebene Pfad wird automatisch entfernt. Die App versucht das Backend unter <SERVERADDRESS>/api zu erreichen. Laufen Backend und App auf der gleichen URL, kann diese Variable weggelassen werden.		✅
⬇️ Server-Variablen			
DB_HOST	URL zur Datenbank		✴️
DB_PORT	Port der Datenbank	5432	✅
DB_NAME	Name der Datenbank		✴️
DB_USERNAME	Nutzername für Zugang zu Datenbank		✴️
DB_PASSWORD	Passwort zum Zugang zur Datenbank		✴️
APPLICATION_SECRET	Zufällige Zeichenkette zur Validierung der Session-Tokens und Kodierung von Passwörtern und Zugangsdaten.		✴️
USE_SECURITY_STRICT_LIMIT	Soll ein Anfrage-Limit für Login, Reset und Co gesetzt werden? In diesem Fall ist der Nutzer nicht angemeldet, sondern versucht es.	true	✅
SECURITY_STRICT_LIMIT _WINDOW	Über welches Zeitfenster soll das Limit angewandt werden? Format: [0-9]*(y|d|h|m|s)	15m	✅
SECURITY_STRICT_LIMIT _REQUEST_COUNT	Wie viele fehlerhafte Anfragen müssen gesendet werden, bis das Limit aktiviert ist?	15	✅

Variable	Zweck	Default	Optional
USE_SECURITY_LIMIT	Soll ein Anfrage-Limit für Anfragen innerhalb der App gesetzt werden? In diesem Fall ist der Nutzer angemeldet.	true	✅
SECURITY_LIMIT_WINDOW	Über welches Zeitfenster soll das Limit angewandt werden? Format: [0-9]*(y|d|h|m|s)	1m	✅
SECURITY_LIMIT_REQUEST_COUNT	Wie viele fehlerhafte Anfragen müssen gesendet werden, bis das Limit aktiviert ist?	500	✅
TRUST_PROXY	Wird der Server hinter einem Proxy betrieben und Rate-Limit verwendet? Ist dieser Wert nicht gesetzt, wird davon ausgegangen, dass kein Proxy verwendet wird. Folgende Werte können gesetzt werden: true / false Anzahl der Proxies: [0-9]* IP-Adresse des Proxy: ip IP-Adressen der Proxy: ip1,ip2,...		✅
⬇️ Database-Variablen			
POSTGRES_DB	Name der Datenbank, die bei Erstellung direkt angelegt wird.		💥
POSTGRES_USER	Benutzername des Users, der bei Erstellung direkt angelegt wird.		💥
POSTGRES_PASSWORD	Passwort zum User, das bei Erstellung gesetzt wird.		💥

💥: Ein Fehlen dieser Variable verhindert das Starten der Anwendung!

Hinweis: Eine fehlerhafte Konfiguration der optionalen oder geforderten Variable verhindert das Starten der Anwendung.
Hinweis: Ist eine Datenbank leer, werden Backups automatisch wiederhergestellt, sollte ein solches existieren.
Hinweis: Das APPLICATION_SECRET wird zur Verschlüsselung von Passwörtern und Zugangsdaten in der Datenbank verwendet. Bei einer Änderung des Secrets kann die Anwendung weder Nutzer-

Zugänge prüfen noch E-Mails für Zugangs-Resets versenden. In diesem Fall muss die Anwendung komplett neu aufgesetzt werden.
Daten können entsprechend über ein Backup wiederhergestellt werden, jedoch werden dabei Zugangsdaten (Credentials) nicht überschrieben oder entfernt. Diese können nur über die Benutzeroberfläche geändert werden, da spezielle Zugänge wie der E-Mail-Versand bei Änderungen validiert werden müssen. Nutzer-Passwörter werden nach einem Backup-Restore nicht zurückgesetzt, um Fremdzugriffe zu verhindern.
In einem Fall, bei dem Zugangsdaten nicht mehr stimmen und der Mailversand nicht klappt, muss die Anwendung neu aufgesetzt werden.

2.5 Update der Version

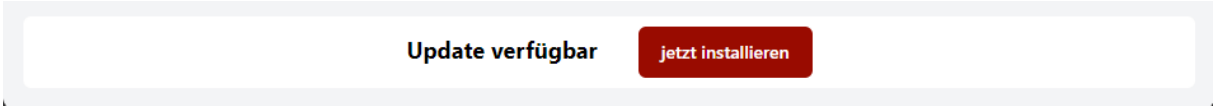
Um eine Version auf eine Neuere zu aktualisieren, muss meist nur der Docker-Tag oder das Repo ersetzt werden.
Wer Docker mit `latest` nutzt, kann das neue Image direkt mit `docker pull` neu beziehen und dann den Container neustarten.

Informationen zu neuen Versionen können innerhalb der App unter `Benutzer > Version` oder in den Release-Pages gefunden werden.
Die Releases beinhalten Informationen zu einem Update und was zu beachten ist. So enthalten die Release-Informationen beispielsweise Vorbereitungen vor einem Update.

Bei Verwendung mittels Git, müssen die Repos neu bezogen werden. Anschließend müssen die Dependencies neu installiert und die Anwendungen neu gebaut werden.

2.6 WebApp

FF Operation ist als WebApp verfügbar. Dadurch lässt sich die Anwendung auf einem Smartphone oder Desktop über den Browser installieren.
Sollte die Version des FF Operation aktualisiert werden, wird dem Nutzer in der Anwendung eine Information angezeigt, dass die Anwendung aktualisiert werden kann.

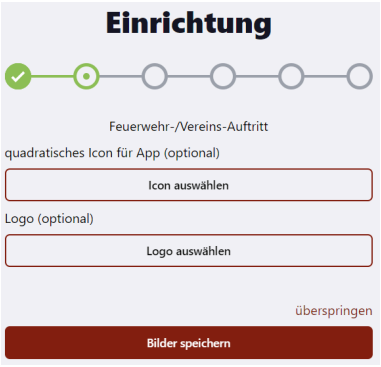


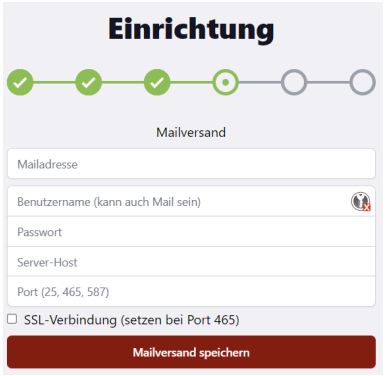
2.7 Einrichtung

Um die Anwendung nutzen zu können, kann ein erster Administrator-Account wie folgt erstellt werden:

Admin Benutzer erstellen: Um einen ersten Benutzer mit Administrator-Berechtigungen zu erstellen, muss der Einrichtungs-Assistent unter dem Pfad `/setup` aufgerufen werden. Nach der initialen Einrichtung wird der Pfad automatisch geblockt. Der Nutzer, welcher über die Einrichtung erstellt wird, wird anschließend als `Owner` gekennzeichnet und hat unabhängig der gesetzten Berechtigungen Vollzugriff auf die gesamte Anwendung.

Der Einrichtungs-Assistent ermöglicht das Setzen erster Einstellungen wie Vereinsdaten und Logos. Auch ermöglicht der Assistent das Einrichten der Mail-Adresse, die von FF Operation verwendet werden soll. Über diese Mailadresse können andere Nutzer eingeladen, Zugänge zurückgesetzt oder Newsletter versendet werden.





Rollen und Berechtigungen: Unter `Verwaltung > Rollen` können die Rollen und Berechtigungen für die Benutzer erstellt und angepasst werden.

Nutzer einladen: Unter `Verwaltung > Benutzer` können weitere Nutzer eingeladen werden. Diese erhalten dann eine E-Mail mit einem Link. Über diesen Link können die Nutzer einen Account mit Zugangsdaten erstellen. Für den Zugang können entweder TOTP oder Passwörter verwendet werden.

3 Konzepte

FF Operation basiert auf mehreren Konzepten, die das System modular und flexibel machen, so dass es an verschiedene Anwendungsfälle angepasst werden kann.

3.1 Stammdaten

Stammdaten sind grundlegende Basisdaten, die als Grundlage für weitere Einträge dienen. Dazu gehören z.B. die Eintragsart wie Einsatz/Übung... oder die auswählbaren Kräfte, Fahrzeuge und co..

Diese Daten sind frei definierbar, so dass die Benutzer ihre eigene Namensgebung festlegen und sicherstellen können, dass alle benötigten Einträge zur Verfügung stehen.

Damit Einträge wie Einsätze angelegt oder verwendet werden können, müssen **zuvor** die entsprechenden Stammdaten angelegt worden sein.

3.2 Berechtigungen

Das Berechtigungssystem ist tief in FF Operation integriert und steuert den Zugriff von Benutzern oder API-Clients auf verschiedene Sektionen und Module. Berechtigungen bestimmen, ob jemand Daten lesen, erstellen, aktualisieren oder löschen kann.

Berechtigungen werden immer summiert:
Ein Benutzer erhält alle Berechtigungen, die ihm direkt oder indirekt über Rollen zugewiesen wurden.
Ein Beispiel: Erhält ein Nutzer Leserechte zu den Mitgliedern über eine Rolle aber auch Rechte zum Erstellen direkt zugewiesen, so kann der Benutzer letztendlich Mitglieder erstellen. Die höhere Berechtigung zählt in dem Fall.

Der Berechtigungseditor ist in Sektionen und Module unterteilt. Wenn ein Benutzer eine Berechtigung für einen Abschnitt erhält, gilt diese automatisch auch für alle untergeordneten Module.

Hinweis: Um Einträge in einem Modul, das auf Stammdaten zugreift, anlegen oder bearbeiten zu können, erhält der Benutzer automatisch Leserechte auf die Stammdaten. Dies bedeutet jedoch nicht, dass der Benutzer die Stammdaten direkt in der Anwendung sehen kann - hierfür benötigt er eine explizite Berechtigung für den entsprechenden Abschnitt oder das entsprechende Modul.

3.3 Zeitformate

Es gibt verschiedene Formate für Zeitangaben. Das eine Format wird für Einstellungen wie der Session-Gültigkeitsdauer, das andere für wiederkehrende Termine und Erinnerungen verwendet.

3.3.1 Gültigkeitsdauer

Angaben im Format **<zahl>(mins|hrs|days|weeks|months|yrs|m|h|d|w|mo|y)** definieren sich durch eine Zahl gefolgt von einer Zeiteinheit und beschreiben Zeitlängen.
Die unterstützten Zeiteinheiten sind:

- **m** bzw. **mins**: Minuten - Beispiel: **15m** bzw. **15mins** für 15 Minuten gültig
- **h** bzw. **hrs**: Stunden - Beispiel: **2h** bzw. **2hrs** für 2 Stunden gültig
- **d** bzw. **days**: Tage - Beispiel: **1d** bzw. **1days** für 1 Tag gültig
- **w** bzw. **weeks**: Minuten - Beispiel: **15w** bzw. **15weeks** für 3 Wochen gültig
- **mo** bzw. **months**: Monate - Beispiel: **1mo** bzw. **1months** für 1 Monat gültig
- **y** bzw. **yrs**: Minuten - Beispiel: **15y** bzw. **15yrs** für 15 Jahre gültig

Dieses Format wird hauptsächlich für die Gültigkeitsdauer von Nutzersessions verwendet.

3.3.2 Zeitintervalle

Angaben im Format **<zahl>-(d|m|y)** oder **DD/MM** oder **DD/*** beschreiben Zeitintervalle.

Format	**als Intervall**	**als Erinnerung**
<zahl>-(d|m|y)	Intervall für alle x Tage, alle x Monate oder alle x Jahre. z.B.: **7-d** für alle 7 Tage	Erinnerung für x Tage, x Monate oder x Jahre vor dem Fälligkeitsdatum.
DD/MM	Intervall für jedes Jahr an einem festen Tag. z.B.: **15/06** für den 15. Juni	Erinnerung an einem bestimmten Tag vor dem Fälligkeitsdatum.
DD/*	Intervall für bestimmten Tag jeden Monat. z.B.: **01/*** für den ersten Tag jeden Monat	Erinnerung an einem bestimmten Tag eines Monat vor dem Fälligkeitsdatum.

Dieses Format wird hauptsächlich für die Intervalle von Wartungen und Prüfungen und den Zeitpunkt der Erinnerung vor dem nächsten Check verwendet.

3.4 Engines

FF Operation stellt eine Reihe von systemweiten Funktionen zur Verfügung, die vom Benutzer konfiguriert und in verschiedenen Modulen verwendet werden können.

3.4.1 Notification-Engine

Die Notification-Engine ermöglicht es dem Benutzer, Benachrichtigungen für verschiedene Ereignisse in der Anwendung zu konfigurieren. Dies umfasst sowohl systemweite Vorgänge als auch Erinnerungen an Fristen und Fälligkeiten.
Benachrichtigungen können entweder direkt in der Anwendung angezeigt oder per E-Mail erhalten werden. Der Benutzer kann dabei selbst festlegen, welche Ereignisse auf welchem Weg mitgeteilt werden sollen.
Dabei kann ein Nutzer nur Benachrichtigungen für Module konfigurieren, für die er über entsprechende Berechtigungen verfügt. Werden einem Nutzer nachträglich Berechtigungen entzogen, prüft das System beim Versand einer Benachrichtigung automatisch, ob der Zugriff auf das betreffende Modul weiterhin besteht.

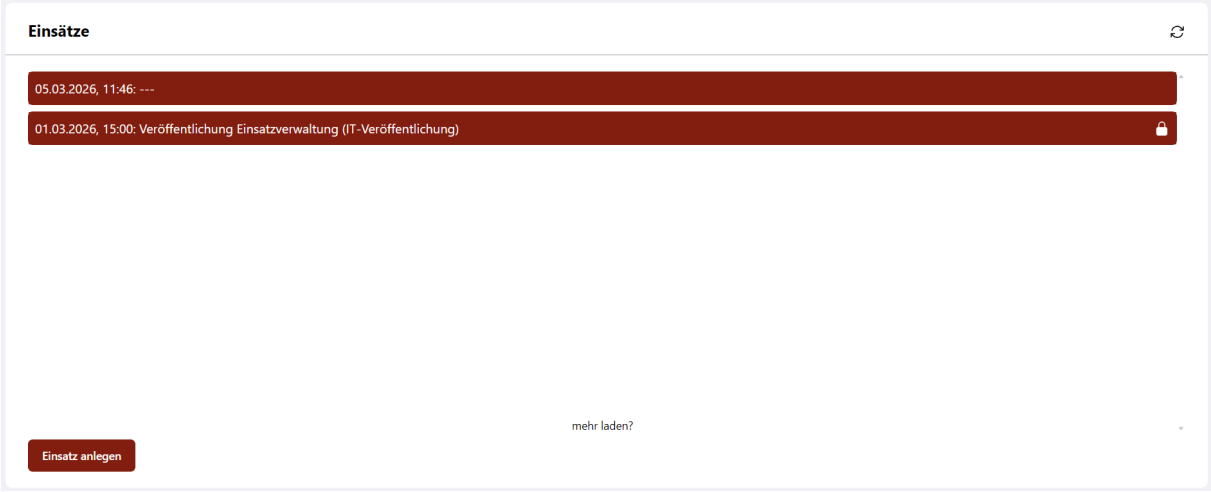
Eine detaillierte Anleitung zur Verwendung finden Sie unter **Benutzerbereich und Accounteigenschaften -> Benachrichtigungen** (Abschnitt 5.2).

4 Module

FF Operation nutzt verschiedenste Module, um Daten zu organisieren, die Verwaltung zu vereinfachen und Berechtigungen sinnvoll setzen zu können.
Diese Module ermöglichen die Anpassung der Anwendung an die eigenen Bedürfnisse, sodass die Daten der Feuerwehr oder des Vereins optimal abgebildet werden können.

Die Module gliedern sich in drei Teilbereiche, die sich an der Navigationsleiste orientieren:
- Zum einen die Verwaltung der Einsatze mit dem Formular zur Dateneingabe.
- Die übrigen Teilbereiche dienen der Verwaltung von Basisdaten wie Gerätschaften, Fahrzeuge oder Kleidung sowie der Konfiguration und Steuerung der Anwendung selbst.

4.1 Einsatzdaten und Dokumentation

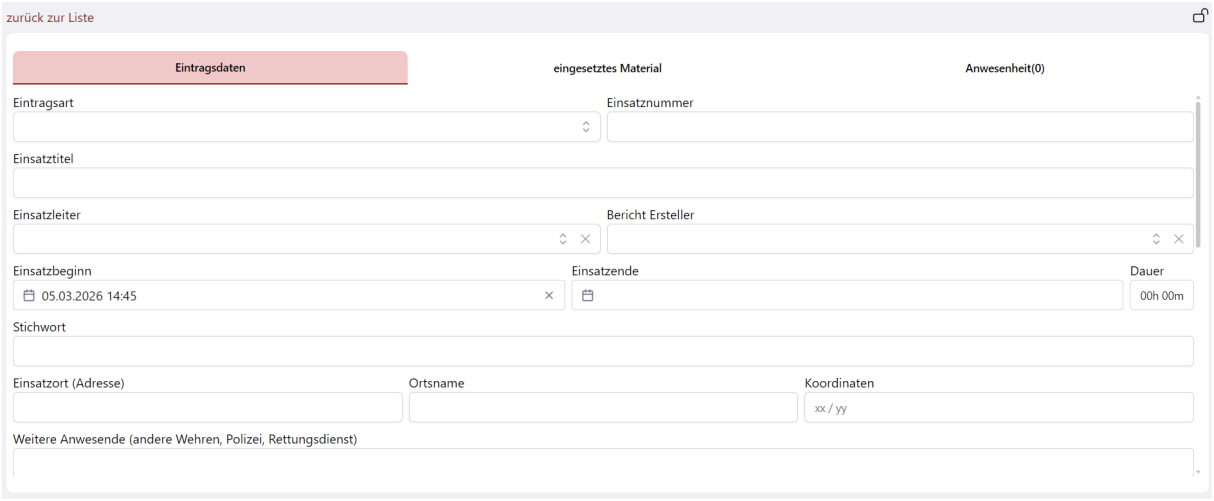


Das Modul Einsätze zeigt alle aktuell laufenden und abgeschlossenen Einsätze an. Neue angelegte Einsätze werden automatisch an alle aktiven Geräte übermittelt und die Liste aktualisiert.
Ein Reload-Button oben rechts ermöglicht das manuelle Neuladen.
Ein Schloss-Symbol kennzeichnet schreibgeschützte Einträge - diese können geöffnet, aber nicht bearbeitet werden.
Die Liste nutzt infinite Loading: Beim Scrollen nach unten werden weitere Einträge geladen. Über Berechtigungseinstellungen lässt sich die Anzahl der angezeigten Einträge und die Tiefe der Historie begrenzen.

Die Daten zu den Einträgen sind aufgeteilt in Eintragsdaten, eingesetztes Material und Anwesenheit. Alle Daten der Einträge sind kollaborativ verfügbar. Daten werden auch nachsynchronisiert, wenn ein Gerät zwischenzeitlich die Internetverbindung verliert und währendessen der Browser **nicht** neugeladen wird. Ein Neuladen der Seite kann auch passieren, wenn das Gerät vorübergehend im Standby ist.

4.1.1 Eintragsdaten

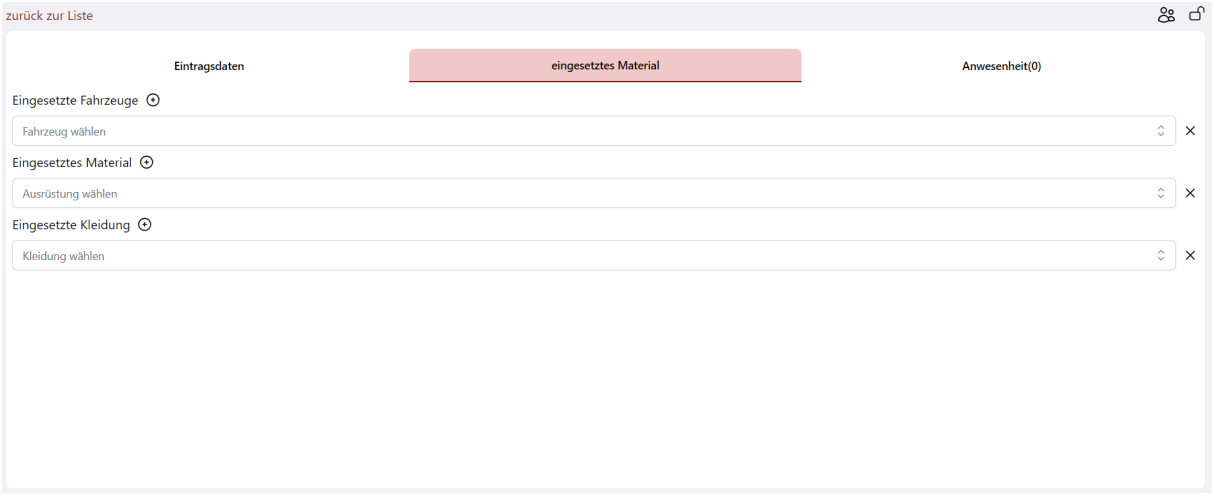
Wird ein Einsatz neu angelegt, beinhaltet dieser bis auf das Startdatum keine weiteren Daten. Anhand des gesetzten Enddatums werden alle verfügbaren Kräfte, Geräte etc. ermittelt.



Das Datenformular beinhaltet Felder zur Eingabe von typischerweise benötigten Feldern. Sind am Feld hinten Pfeile, so wird von diesen DropDowns auf konfigurierten Basisdaten zugegriffen. Die Eingabe zum Datum kann durch tippen oder über das angezeigte Dialogfeld erfolgen. Auf mobilen Geräten wird die Eingabe für das Datum aus Usabilitygründen zentral angezeigt.

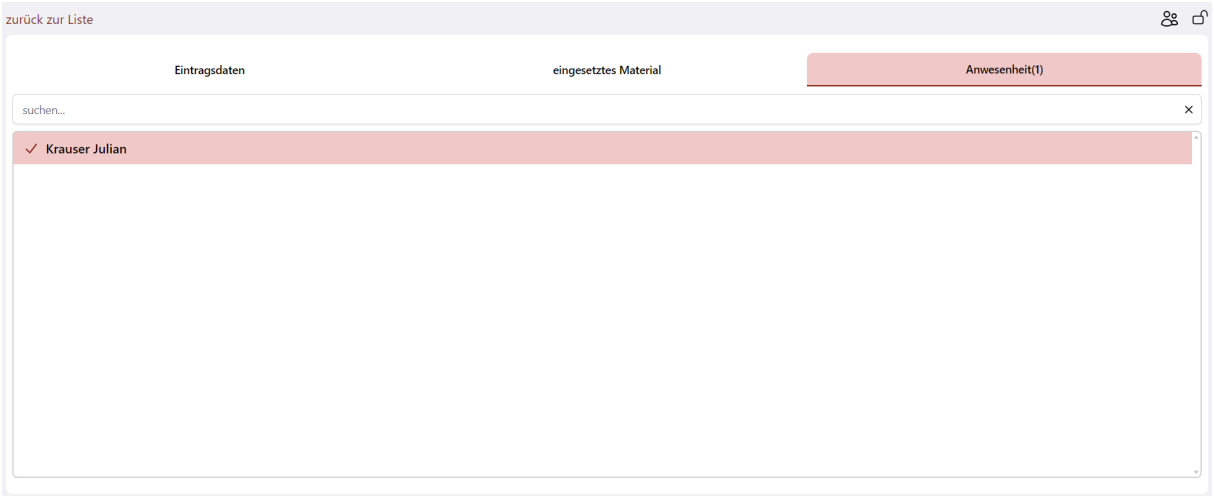
Das Formular hat außerdem ein Freitexteditor, welcher Daten zum Eintrag erfassen kann. Auch gibt es einen separaten Abschnitt zur Erfassung von Kontaktpersonen mit deren Beteiligung und Daten.

4.1.2 eingesetztes Material



Der Tab „eingesetztes Material“ erfasst Daten zu den verwendeten Gerätschaften, Fahrzeugen und Kleidung. Je nach Eintrag werden unterschiedliche Daten abgefragt. So zum Beispiel, den Fahrer oder von wem etwas verwendet wurde. Alle Einträge können mit Notizen versehen werden.

4.1.3 Anwesenheit



Im Tab „Anwesenheit“ kann die Anwesenheit der verfügbaren Kräfte erfasst werden. Über die Suche kann zusätzlich die Übersicht gefiltert werden. Wird eine Kraft irgendwo im Formular ausgewählt, wird diese automatisch auch in der Anwesenheit angehackt.

4.1.4 Sperren, Freischalten und Löschen

Die Icons im rechten oberen Eck ermöglichen das Sperren, Freischalten oder Löschen eines Eintrags. Diese Icons werden abhängig von denBerechtigungen und dem aktuellen Status des Eintrags angezeigt.

Schloss offen: Der aktuell geöffnete Eintrag kann für die Bearbeitung gesperrt werden. Für alle Nutzer werden die Felder auf Readonly umgestellt. Jegliche Änderungen werden vom Server blockiert.

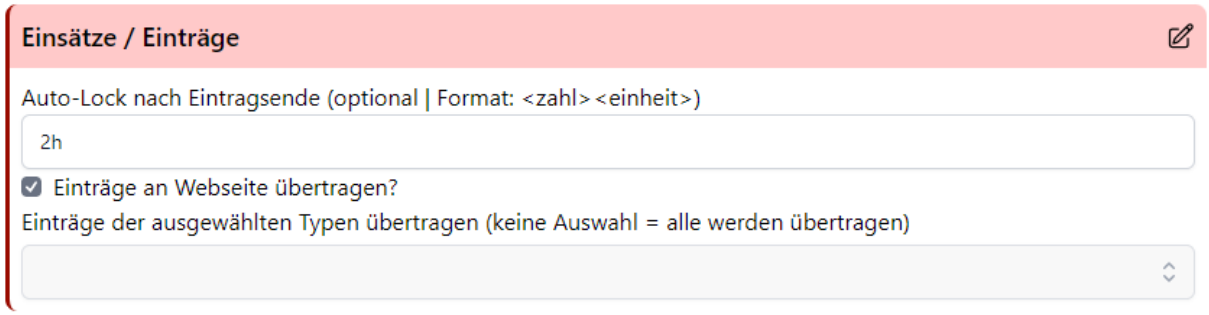
Schloss geschlossen: Der aktuelle Eintrag ist im Modus Readonly. Dies ist der Fall, wenn ein Nutzer keine Berechtigungen zum Bearbeiten hat oder der Eintrag selbst Readonly ist.

Schlüssel: Über den Schlüssel kann ein Eintrag wieder zum Bearbeiten freigeschalten werden. Dazu muss ein Nutzer Admin-Rechte haben.

Mülltonne: Der aktuelle Eintrag kann über die Mülltonne gelöscht werden. Das Icon wird nur angezeigt, wenn der Nutzer die Berechtigung zum Löschen hat und der Eintragsbeginn geleert ist. Da ein Eintrag standardmäßig mit Beginn erstellt wird, wird das Icon standardmäßig nicht angezeigt.

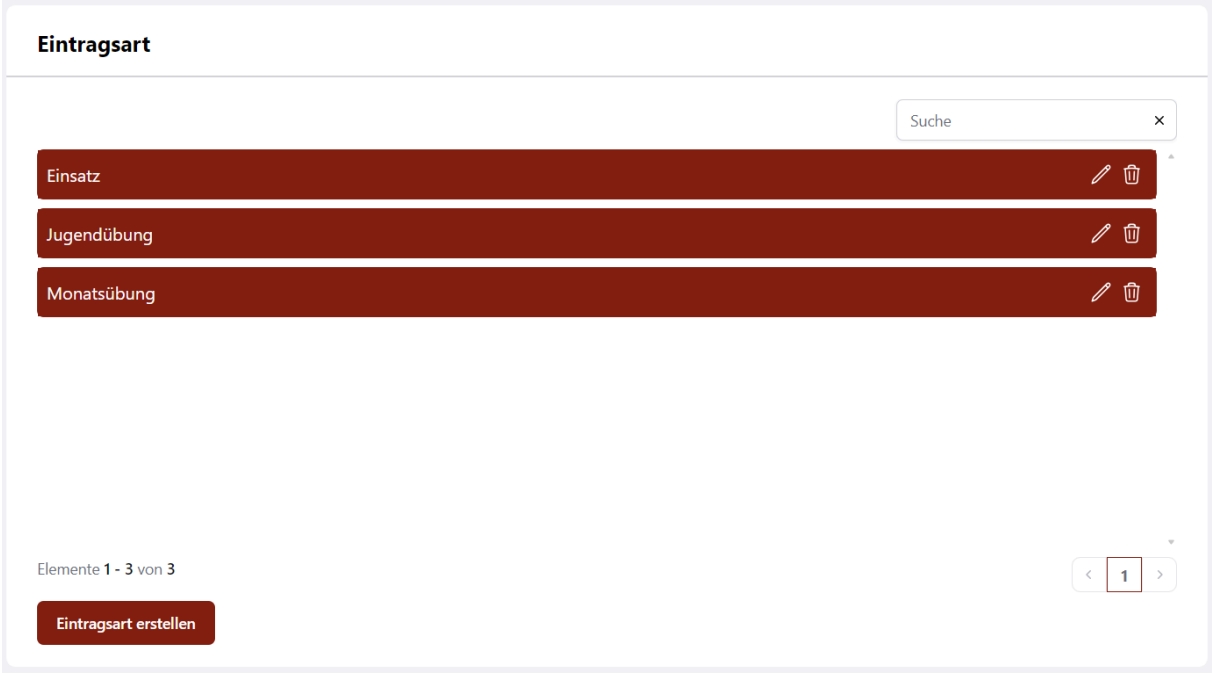
4.1.5 Synchronisierung mit FF Webpage

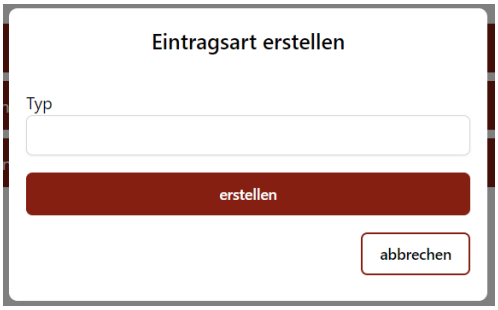
In den Modulspezifischen Einstellungen (Abschnitt 4.12) kann ein automatischer sync mit FF Webpage eingerichtet werden.



Für die Synchronisierung muss zusätzlich die Moduleinstellung `Webpage WebAPI Connect` eingerichtet sein. Wird die Synchronisierung für die Einträge aktiviert, kann zusätzlich noch ausgewählt werden, ob alle angelegten oder nur ausgewählte Eintragsarten synchronisiert werden sollen.

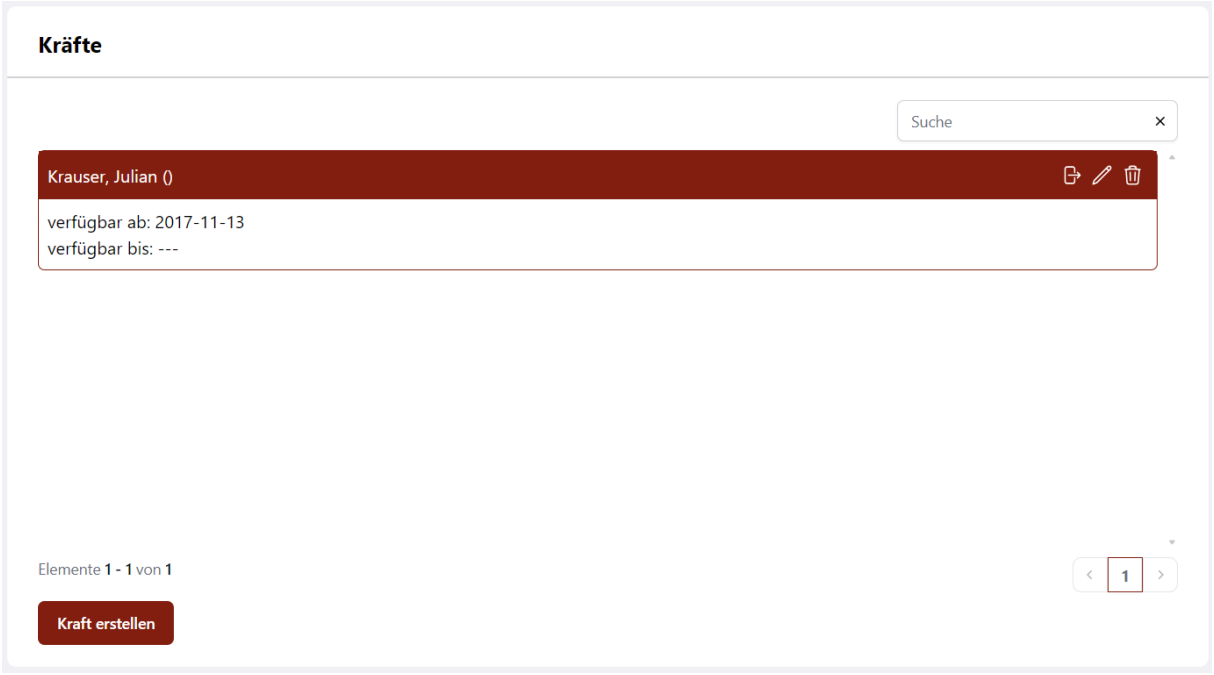
4.2 Eintragsart

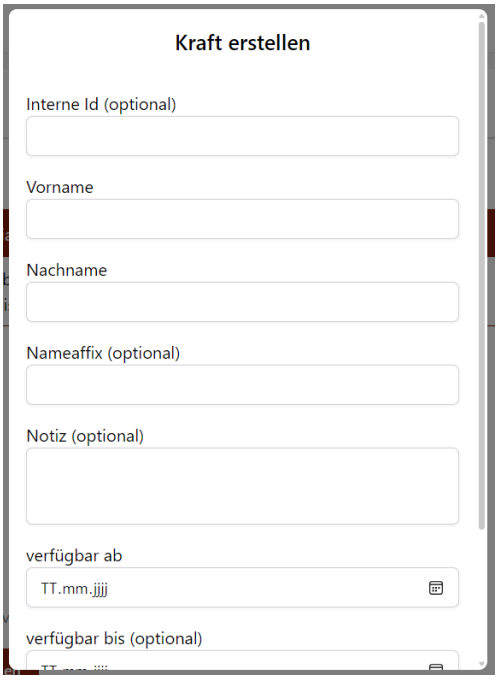




Eintragsarten kategorisieren die Einträge. So kann hierüber zwischen z.B. Einsätzen, Übungen und co unterschieden werden.
Eintragsarten bestehen nur aus einer Bezeichnung.

4.3 Kräfte



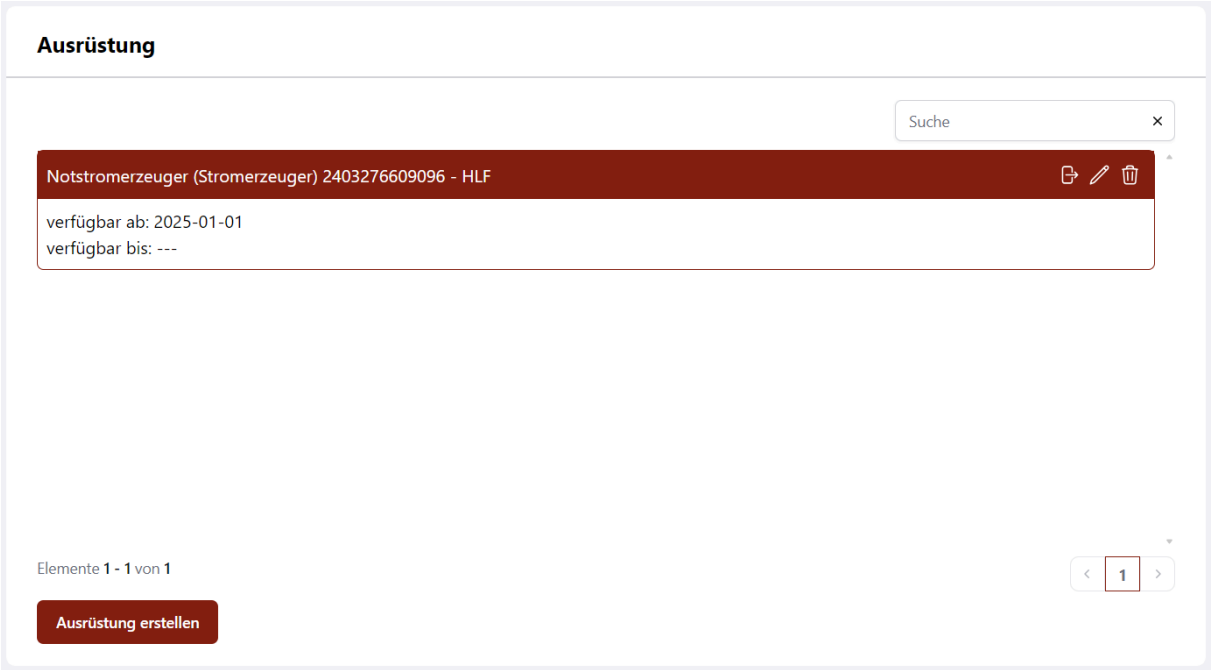


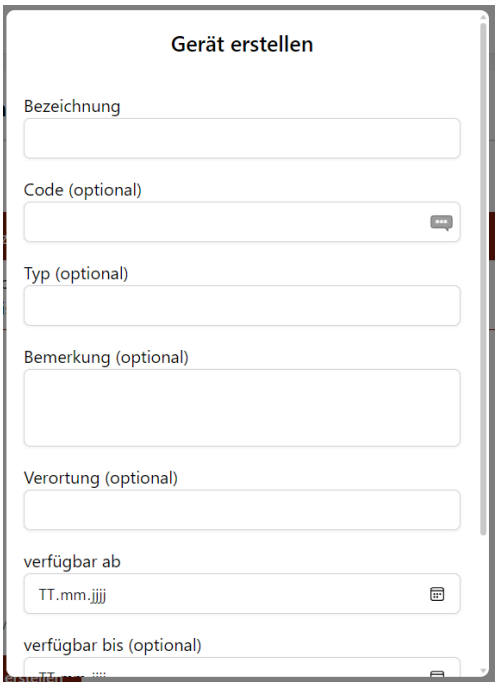
Kräfte, auch Mitglieder der Wehr, können für die Anwesenheit oder belegten Positionen ausgewählt werden. Kräfte besitzen Basisinformationen und einen Verfügbarkeitszeitraum.

Bei der Synchronisierung aus FF Admin werden alle Daten übernommen. Bei der Synchronisierung werden auch nicht mehr verfügbare Kräfte entsprechend markiert.

Werden Kräfte manuell erfasst, können diese über das Symbol (siehe rechts) auf verfügbar bis heute gesetzt.

4.4 Ausrüstung



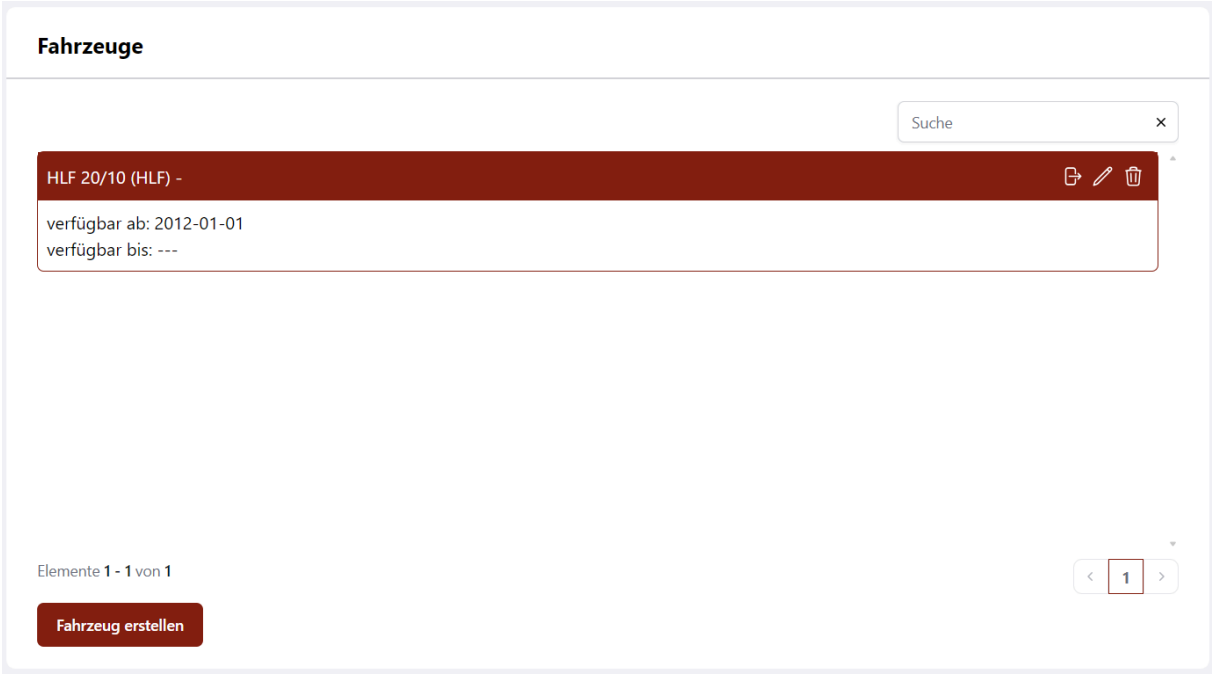


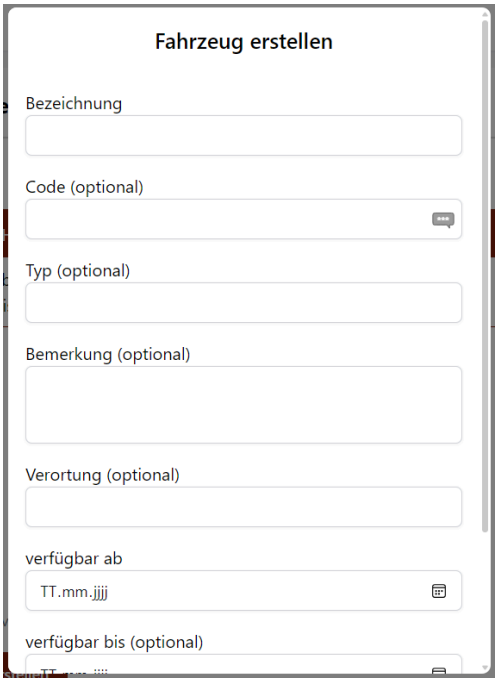
Ausrüstung kann bei eingesetztes Material ausgewählt werden. Ausrüstung besitzt Basisinformationen und einen Verfügbarkeitszeitraum.

Bei der Synchronisierung aus FF Admin werden alle Daten übernommen. Bei der Synchronisierung werden auch nicht mehr verfügbare Geräte entsprechend markiert.

Wird Ausrüstung manuell erfasst, können diese über das Symbol (siehe rechts) auf verfügbar bis heute gesetzt.

4.5 Fahrzeuge



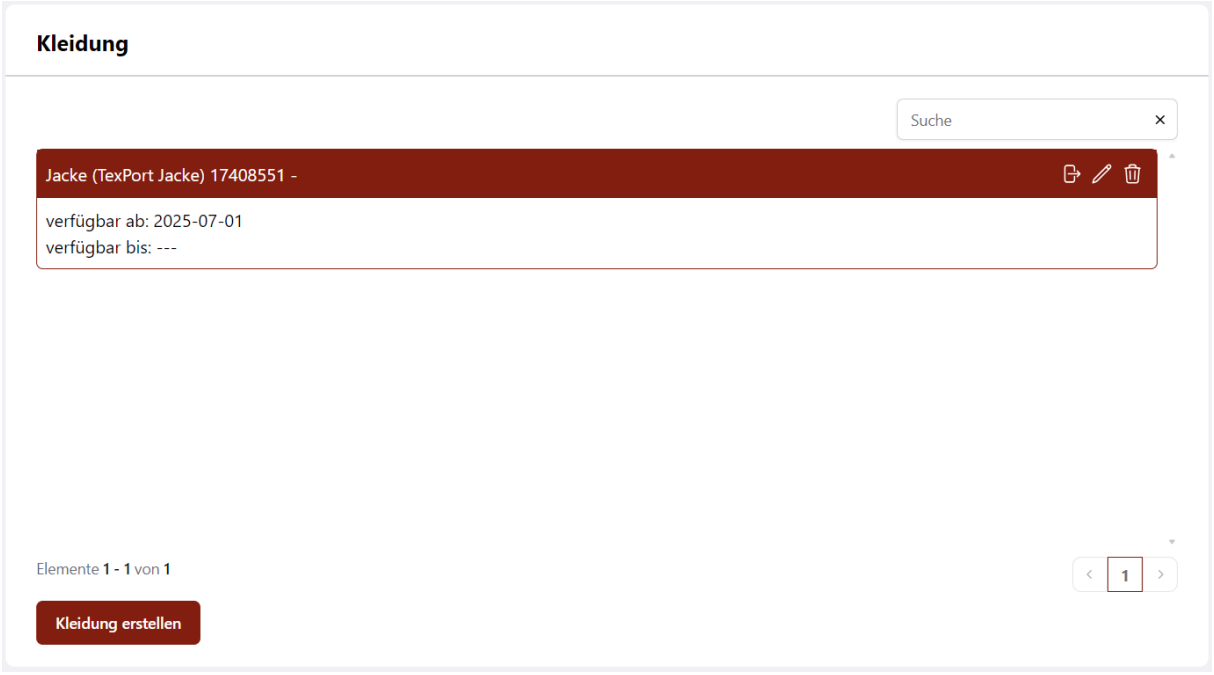


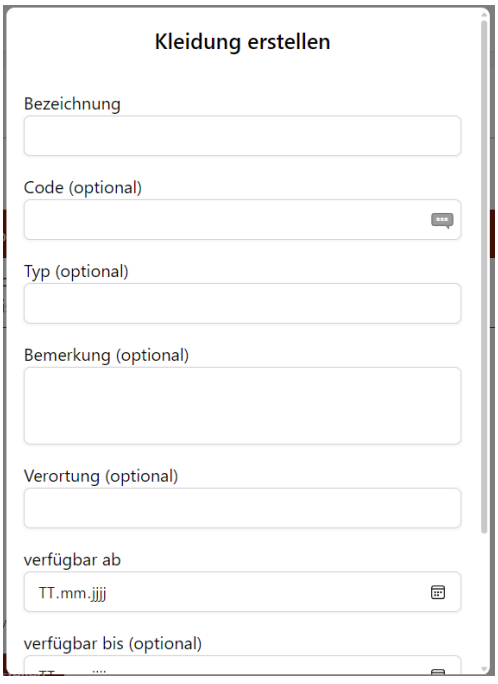
Fahrzeuge können bei eingesetztes Material ausgewählt werden. Ein Fahrzeug besitzt Basisinformationen und einen Verfügbarkeitszeitraum.

Bei der Synchronisierung aus FF Admin werden alle Daten übernommen. Bei der Synchronisierung werden auch nicht mehr verfügbare Fahrzeuge entsprechend markiert.

Wird ein Fahrzeug manuell erfasst, können diese über das Symbol (siehe rechts) auf verfügbar bis heute gesetzt.

4.6 Kleidung



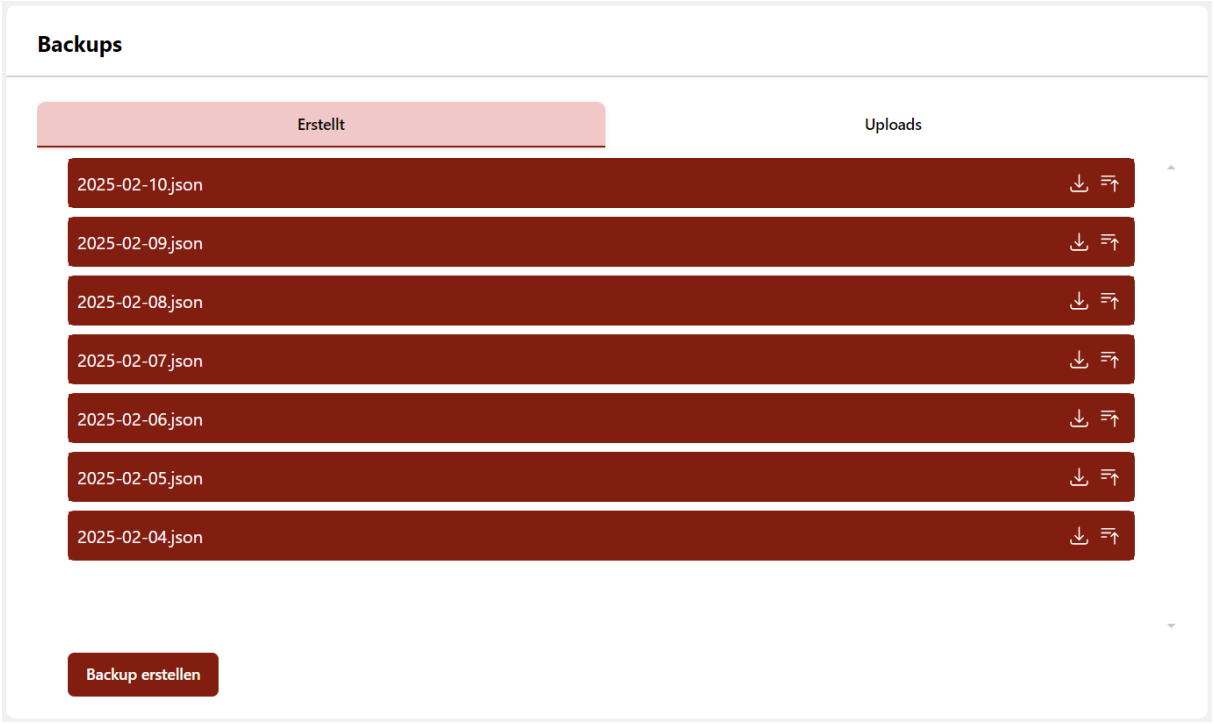


Kleidung kann bei eingesetztes Material ausgewählt werden. Kleidung besitzt Basisinformationen und einen Verfügbarkeitszeitraum.

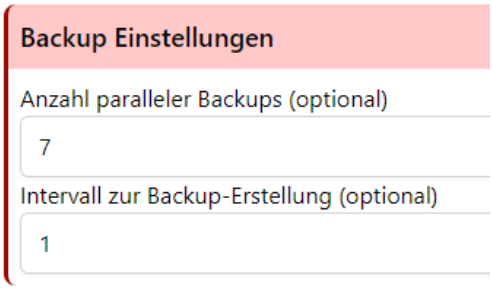
Bei der Synchronisierung aus FF Admin werden alle Daten übernommen. Bei der Synchronisierung werden auch nicht mehr verfügbare Kleidung entsprechend markiert.

Wird Kleidung manuell erfasst, können diese über das Symbol (siehe rechts) auf verfügbar bis heute gesetzt.

4.7 Backups



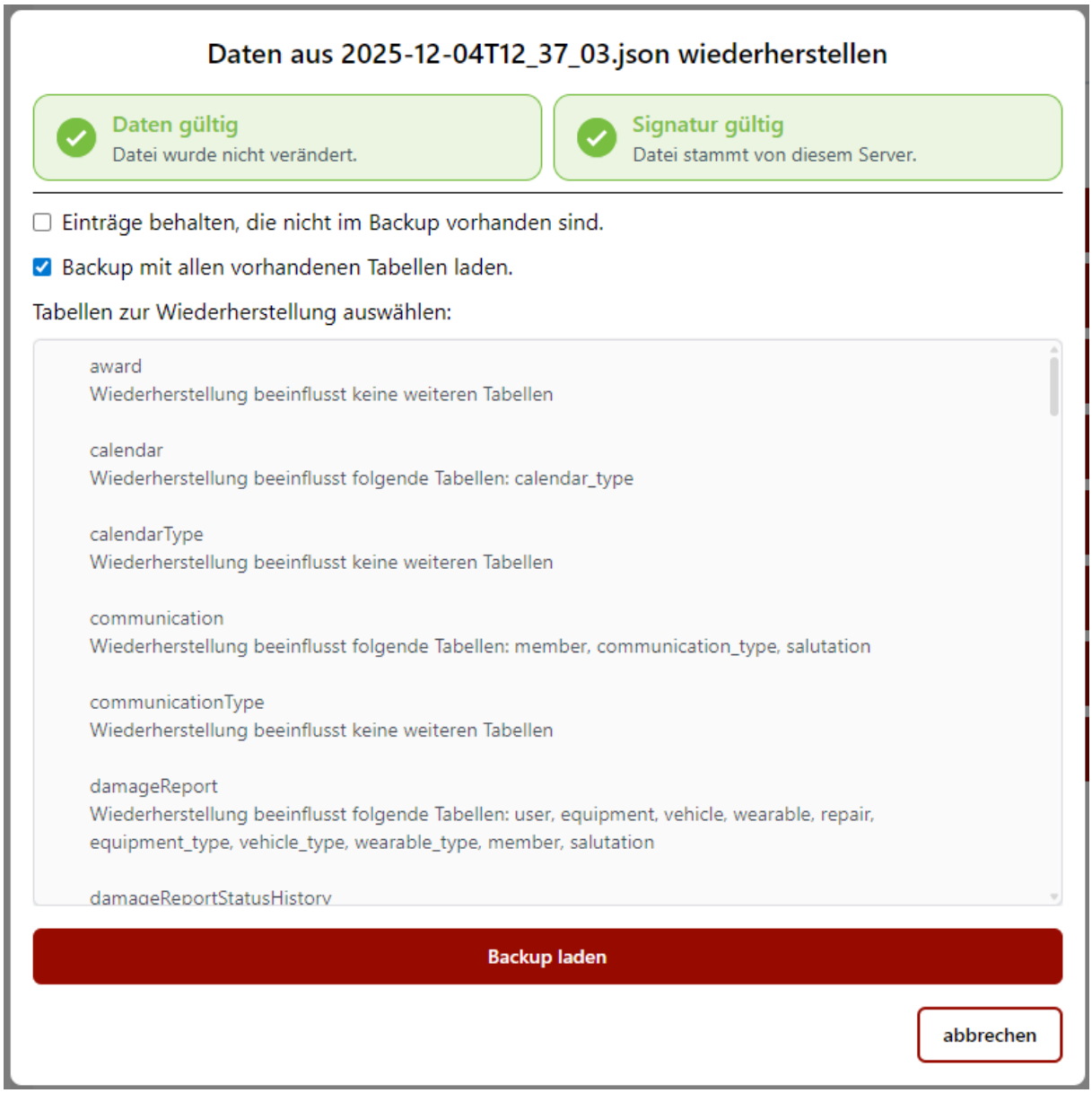
Backups sind automatisch gesicherte Datenstände der Anwendung, die jederzeit wiederhergestellt werden können. Diese Backups sind nicht an eine bestimmte Anwendung gebunden und können daher jederzeit in eine andere Instanz des Admins übertragen werden.



Backups werden in einem festgelegten Intervall erstellt. Das kleinste Intervall beträgt täglich. Zusätzlich kann konfiguriert werden, wie viele Backups parallel zur Verfügung stehen sollen. Standardmäßig ist eine Anzahl von 7 eingestellt, d.h. die gespeicherten Backups reichen immer eine Woche in die Vergangenheit. Die Anzahl bezieht sich dabei nicht auf die Anzahl an Backups im System, sondern auf die Anzahl Tage, an denen ein Backup gemacht wurde. Heißt, dass 2 Backups des selben Tages als eines gewertet wird.
Das Intervall und die Anzahl and Backups, welche parallel gespeichert sein sollen, können in den Einstellungen Abschnitt 4.11 gesetzt werden.

Eine Funktion, die mit den Backups eingeführt wurde, ist `AUTO RESTORE`.
`AUTO RESTORE` ermöglicht die automatische Wiederherstellung des letzten Backups - sofern vorhanden - wenn die Datenbank beim Start des Servers leer ist.

In Version 1.11.0 wurde ein neues Backupsystem eingeführt, welches die Wiederherstellung um einige Optionen erweitert. Durch die Einführung des neuen Systems können alte Backups von vor 1.11.0 nicht wiederhergestellt werden.
Das neue Backup-System führt erweiterte Sicherheits- und Flexibilitätsfeatures ein:



Integrität und Signatur: Jedes Backup enthält eine kryptographische Signatur, die aus dem `APPLICATION_SECRET` entsteht, sowie einen Hash der gespeicherten Daten. Diese ermöglichen die Überprüfung auf nachträgliche Manipulationen. Sollten diese Sicherheitsinformationen fehlen oder ungültig sein, kann das Backup dennoch wiederhergestellt werden, jedoch muss explizit bestätigt werden, dass die Sicherheitshinweise wissentlich ignoriert werden.

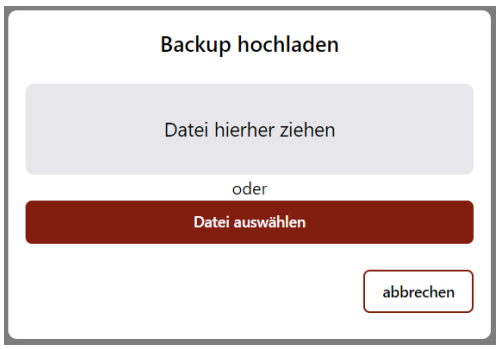
Befindet sich ein manipuliertes Backup im Backup-Ordner des Servers (was nur durch direkte Manipulation auf dem Server möglich ist), schlägt die automatische Wiederherstellung bei leerer Datenbank mit diesem Backup fehl.

Selektive Wiederherstellung: Das System ermöglicht die Wiederherstellung einzelner Tabellen. Dabei werden Daten in verbundenen Tabellen automatisch angepasst - es entstehen ausschließlich zusätzliche Einträge. Löschungen erfolgen nur bei Tabellen-Referenzen, wobei das Backup fehlschlägt, falls Referenzen nicht automatisch aufgelöst werden können. In solchen Fällen müssen alle betroffenen Tabellen zur Wiederherstellung ausgewählt werden.

Inkrementelle Updates: Es können Einträge auf einen älteren Stand zurückgesetzt werden, während neuere Daten erhalten bleiben, welche zum Stand des Backups noch nicht bestanden haben. Daten, welche seit dem Backupzeitpunkt verändert wurden, werden auf den damaligen Stand zurückgesetzt.

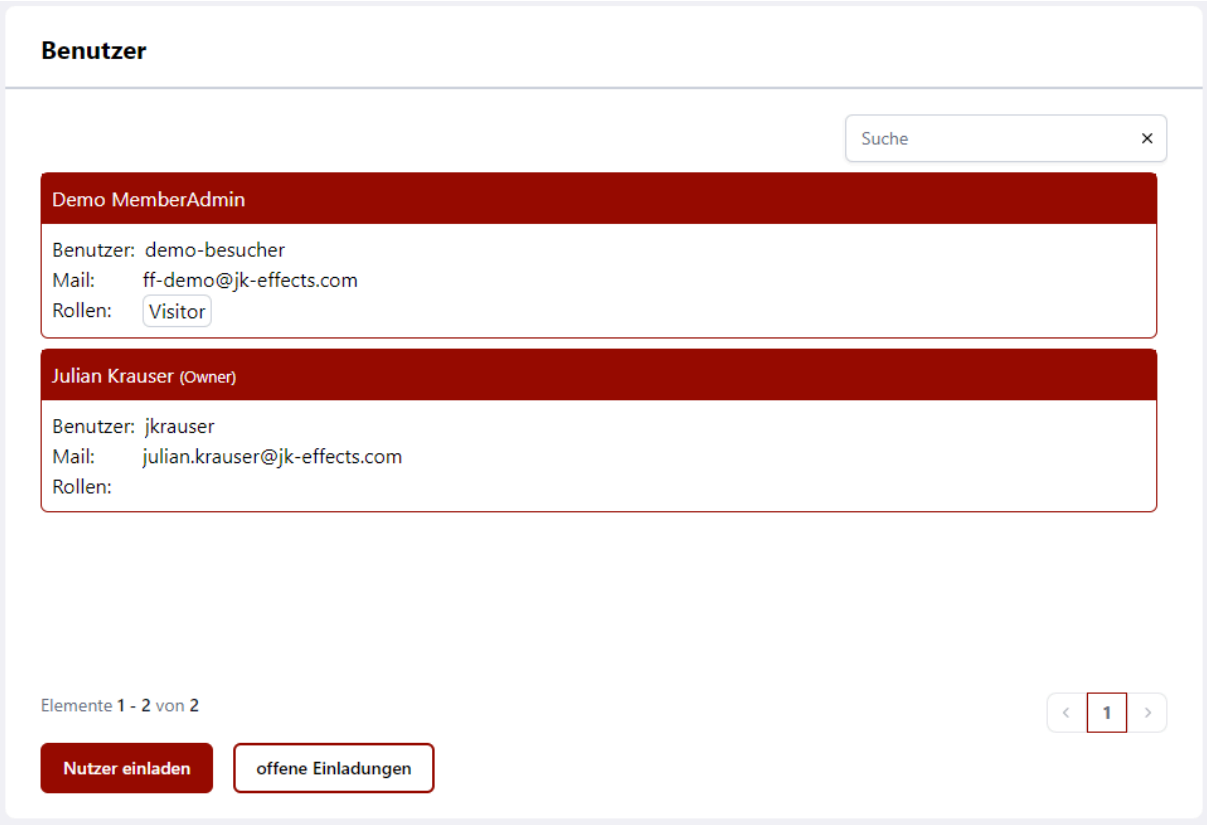
Basisdaten-Integration: Diese Funktionalität ermöglicht die Bereitstellung vorgefertigter Basisdaten als Ausgangspunkt für neue Instanzen. Diese können kontinuierlich mit neueren Versionen aktualisiert werden.

Datenschutz: Alle Zugangsdaten werden verschlüsselt im Backup gespeichert und überschreiben nie bestehende Daten. Bei leeren Datenbanken werden die Zugangsdaten übernommen. Codierte Inhalte werden grundsätzlich nicht bei der Wiederherstellung eines Backups gelöscht. Dadurch werden Zugangsdaten nicht zurückgesetzt und Zugänge gehen nicht verloren. Dies ist besonders wichtig für den Mailversand, da dieser mit falschem Passwort auch ein Reset eines Passworts unmöglich macht. In einem Fall, bei dem Zugangsdaten nicht mehr stimmen und der Mailversand nicht klappt, muss die Anwendung neu aufgesetzt werden.



Heruntergeladene Backups können jederzeit wieder hochgeladen und im Admin gespeichert werden. Im Gegensatz zu den automatisch erstellten Backups sind die Slots nicht begrenzt. Es können also beliebig viele Backups hochgeladen und gespeichert werden.
Es ist geplant, „Backups“ mit Basisdaten zur Verfügung zu stellen. Diese können dann hochgeladen und verwendet werden. Dazu muss allerdings die Funktion der Teil-Wiederherstellung funktionieren, da sonst Daten gelöscht werden.

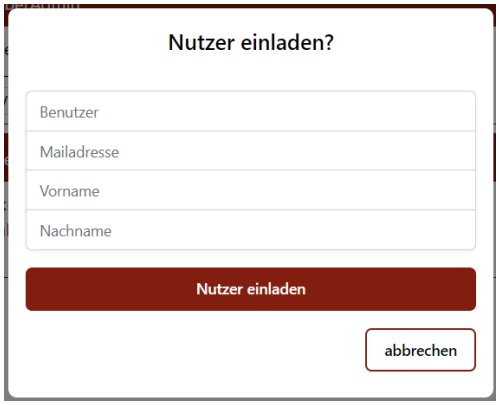
4.8 Benutzerverwaltung



Daten nur von angemeldeten Benutzern geändert werden. Diese Benutzer melden sich mit einem TOTP oder Passwort an. Ein TOTP (Time-based One-time Password) ist ein zeitbasiertes Passwort, das sich jede Minute ändert. Nutzer können außerdem Passkeys (Abschnitt 5.4) für einen schnelleren Login erstellen. Jeder Benutzer hat Lese-, Bearbeitungs- und Löschrechte. Es können auch Rollen erstellt und Benutzern zugewiesen werden.

Benutzer mit dem Status `Owner` haben unabhängig der gesetzten Berechtigungen Vollzugriff auf die gesamte Anwendung.

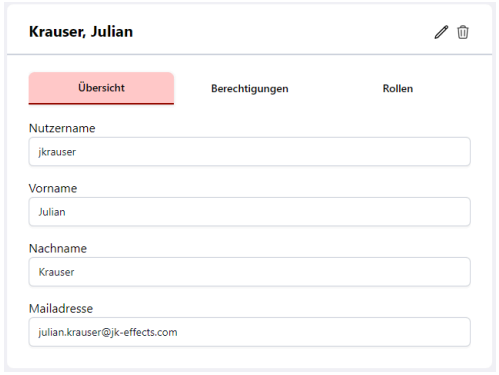
4.8.1 Benutzer einladen



Benutzer können nicht direkt hinzugefügt werden. Eine Einladung muss verschickt werden.
Einladungen sind nur solange gültig, bis sie angenommen oder zurückgezogen werden.
Bei einer Einladung wird ein personalisierter Link an die angegebene E-Mail-Adresse gesendet, über den sich der Benutzer registrieren kann. Nach der Registrierung hat der Benutzer noch keine Rollen oder Berechtigungen. Diese müssen nach der Registrierung zugewiesen werden.
Ein Benutzername oder eine E-Mail-Adresse darf nur einmal existieren.

Wenn ein Benutzer keine Berechtigungen hat oder diese ihm entzogen wurden, wird die Meldung auf der linken Seite angezeigt.
Nach der Registrierung wird diese Meldung standardmäßig angezeigt.
Mit einem Klick auf die Schaltfläche „Jetzt Berechtigungen neuladen“ werden die aktuellen Berechtigungen vom Server abgefragt. Bleibt die Ansicht unverändert, wurden dem Benutzer noch keine Berechtigungen zugewiesen.
Andernfalls erfolgt eine Weiterleitung zur Admin-Oberfläche.

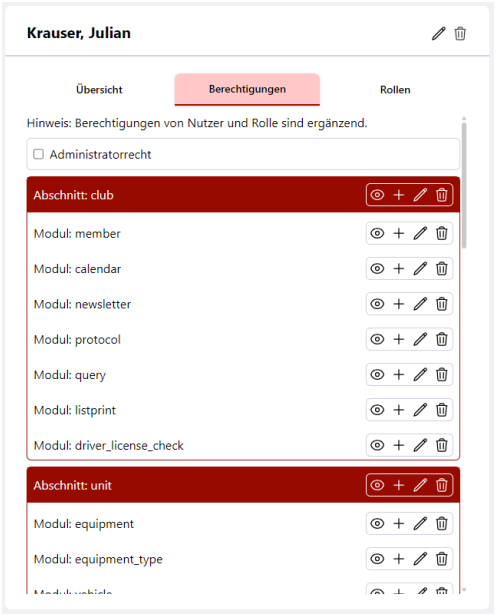
4.8.2 Details



Jeder Benutzer verfügt über einen Benutzernamen, eine E-Mail-Adresse, Vor- und Nachname sowie zugewiesene Berechtigungen und Rollen.
In der Detailansicht können diese Daten eingesehen und bearbeitet werden. Nutzer mit entsprechenden Berechtigungen können dort auch den Benutzernamen ändern.
Wichtig: Bei einer Änderung des Benutzernamens ist anschließend eine Anmeldung per Passwort oder TOTP nicht mehr möglich, sofern der neue Nutzernamen nicht weitergegeben wird. Der Zugang bleibt jedoch über Passkeys erhalten.

4.8.3 Berechtigungen

Berechtigungen werden immer addiert.



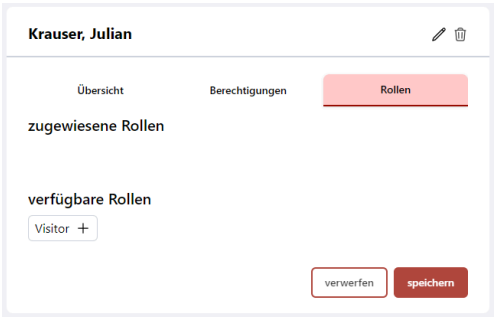
Das heißt: Wenn ein Benutzer direkt zugewiesene Berechtigungen und Rollen erhält, werden die Berechtigungen addiert und der Benutzer kann alles, was diesem direkt zugewiesen wurde und was die Rolle kann.

Das Berechtigungsmodell unterscheidet zwischen Lese-, Erstellungs-, Änderungs- und Löschberechtigungen. Die Berechtigungen sind abgestuft. Das heißt, wer anlegen darf, darf auch lesen. Wer bearbeiten darf, darf auch anlegen und dementsprechend auch lesen usw.

Die Berechtigungen sind entsprechend der Bereiche in der Navigationsleiste gruppiert. Wenn die Berechtigung für einen Abschnitts auf Lesen gesetzt ist, kann der Benutzer mit dieser Berechtigung Daten in allen Modulen des Abschnitts lesen.

Erweiterte Berechtigungen können pro Modul gesetzt werden. Dabei gelten die Berechtigungen des Abschnitts immer mehr als die eines Moduls innerhalb des Abschnitts.

4.8.4 Rollen



Damit Rollen oder Berechtigungen von einem Benutzer vergeben werden können, muss dieser Benutzer über Administratorrechte verfügen. Dabei ist es unerheblich, ob die Admin-Berechtigung über eine Rolle oder direkt vergeben wird.

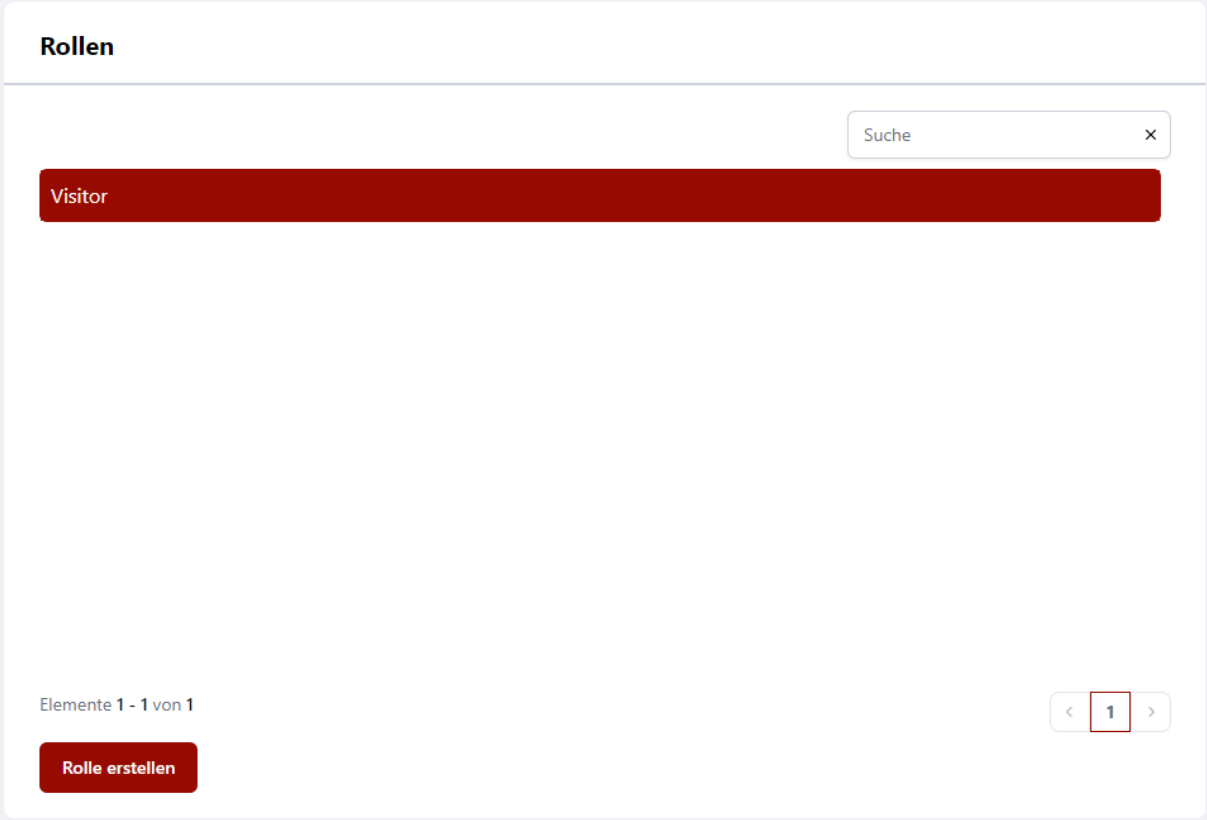
Rollen fassen Berechtigungen zusammen und ergänzen die einem Benutzer direkt zugewiesenen Berechtigungen.

Rollen können sich nicht gegenseitig ausschließen.

Einem Benutzer können mehrere Rollen zugewiesen werden. Muss aber keine Rollen haben.

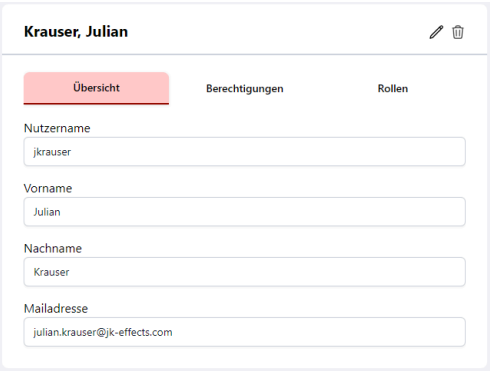
Hinweis: Änderungen an Berechtigungen oder Rollen wirken sich unmittelbar auf die Benutzer aus. Sie werden sofort an die Anwendung übertragen und dort angezeigt, sofern diese beim betroffenen Benutzer geöffnet ist. Ist der Nutzer offline, werden die Änderungen beim nächsten Öffnen der Anwendung übernommen.

4.9 Rollenverwaltung



Rollen dienen der Abstraktion von Berechtigungen. Dadurch können spezifische Berechtigungsschemata direkt einem oder mehreren Benutzern zugewiesen werden, ohne dass diese mehrfach manuell direkt zugewiesen werden müssen.

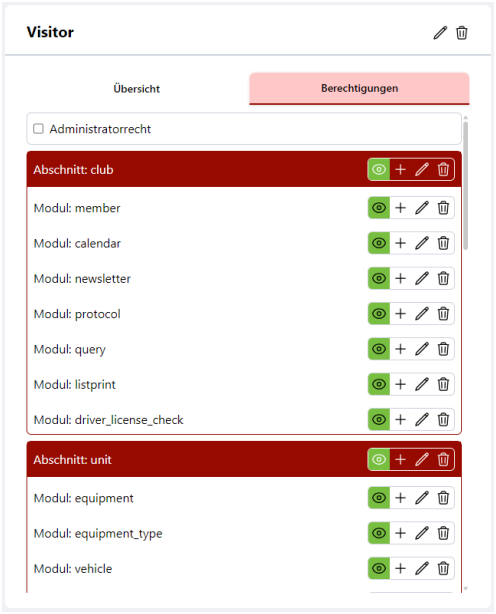
4.9.1 Details



Jede Rolle verfügt über einen Bezeichnung sowie zugewiesene Berechtigungen.
In der Detailansicht können diese Daten eingesehen und bearbeitet werden.

4.9.2 Berechtigungen

Berechtigungen werden immer addiert.



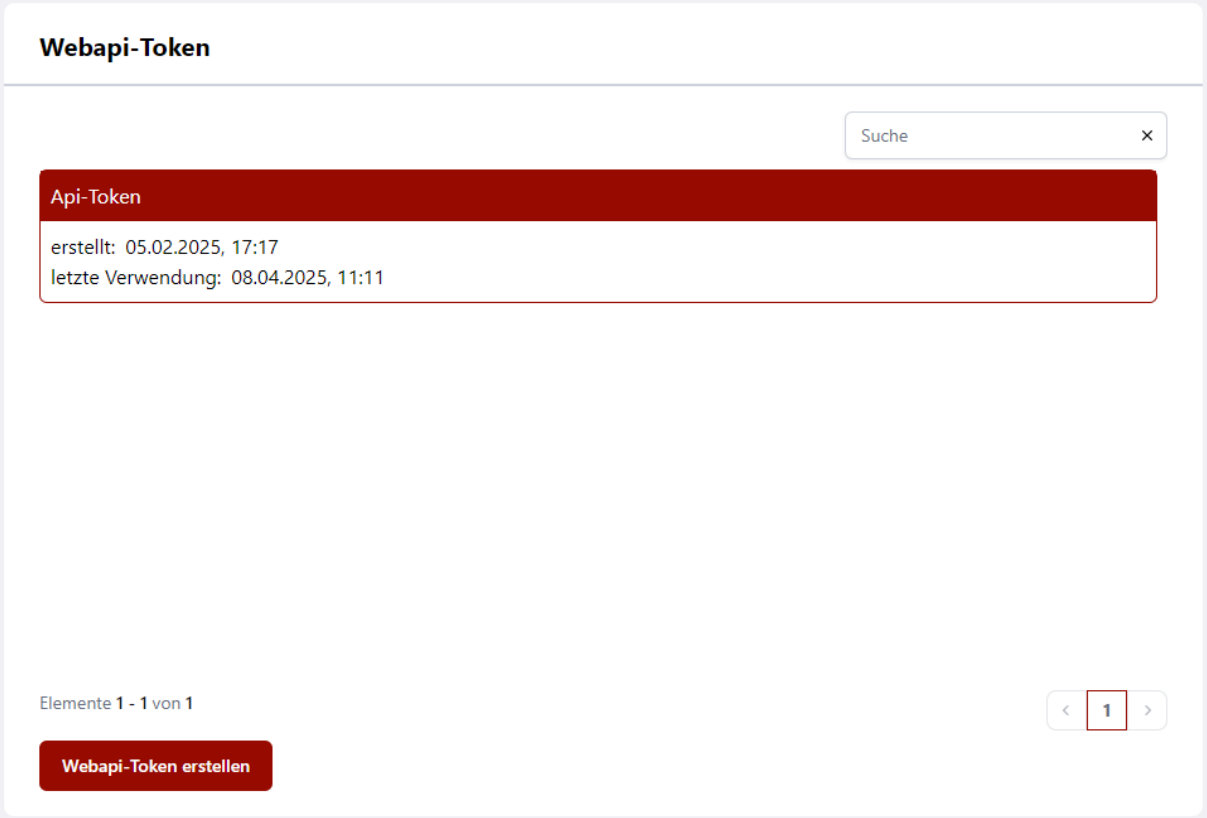
Das heißt: Wenn ein Benutzer mehrere Rollen zugewiesen bekommt, werden die Berechtigungen addiert und der Benutzer kann alles, was die Rollen ermöglichen. Zusätzlich werden auch die nutzerspezifischen Berechtigungen addiert.

Das Berechtigungsmodell unterscheidet zwischen Lese-, Erstellungs-, Änderungs- und Löschberechtigungen. Die Berechtigungen sind abgestuft. Das heißt, wer anlegen darf, darf auch lesen. Wer bearbeiten darf, darf auch anlegen und dementsprechend auch lesen usw.

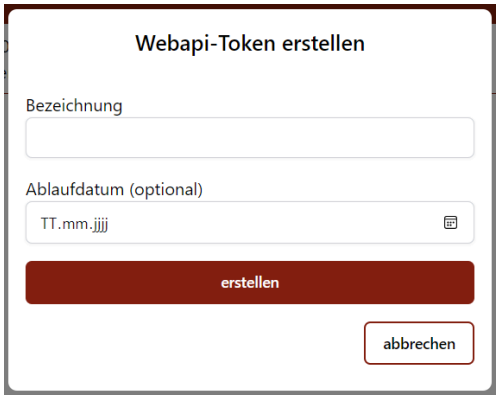
Die Berechtigungen sind entsprechend der Bereiche in der Navigationsleiste gruppiert. Wenn die Berechtigung für einen Abschnitts auf Lesen gesetzt ist, kann der Benutzer mit dieser Berechtigung Daten in allen Modulen des Abschnitts lesen.

Erweiterte Berechtigungen können pro Modul gesetzt werden. Dabei gelten die Berechtigungen des Abschnitts immer mehr als die eines Moduls innerhalb des Abschnitts.

4.10 WebApi



WebApi-Tokens ermöglichen externen Clients oder anderen Anwendungen des FF Ökosystems oder eigenen Anwendungen die Kommunikation mit der Anwendung. Dabei haben WebApis Zugriff auf fast alle Daten der Anwendung, sofern die Berechtigungen gesetzt sind.
Kategorisch ausgeschlossen ist der Zugriff die Anwendungsmodule Backup und WebApi sowie Serverinformationen wie z.B. die Version.

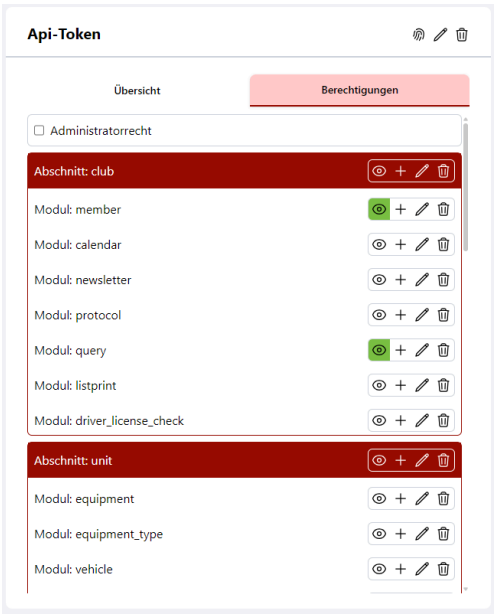


Eine WebApi kann mit einem Verfallsdatum erstellt werden. Dieses Ablaufdatum wird fest eingestellt, wenn eine WebApi Zugriff anfordert.
Zusätzlich wird für jede WebApi ein Token erstellt, das zur Authentifizierung der WebApi verwendet werden kann.

4.10.1 Details

Jede WebApi verfügt über eine Bezeichnung und ein Verfallsdatum.
In der Detailansicht können diese Daten eingesehen und bearbeitet werden.
Wichtig:
Bei einer Änderung der Berechtigungen werden die Berechtigungen erst übernommen, wenn das Zugangs-Token (siehe unten Abschnitt 4.10.3) neu ausgestellt wird. Das Intervall, in dem das Token erneuert wird, ist die `JWT-Gültigkeitsdauer`, welche in den Einstellungen (Abschnitt 4.11) gesetzt werden kann.
Unter dem Fingerabdruck-Symbol kann das Token der WebApi abgerufen werden.
Diese Token sind JWTS und können daher ohne Kenntnis der Serverkonfiguration nicht gefälscht werden.

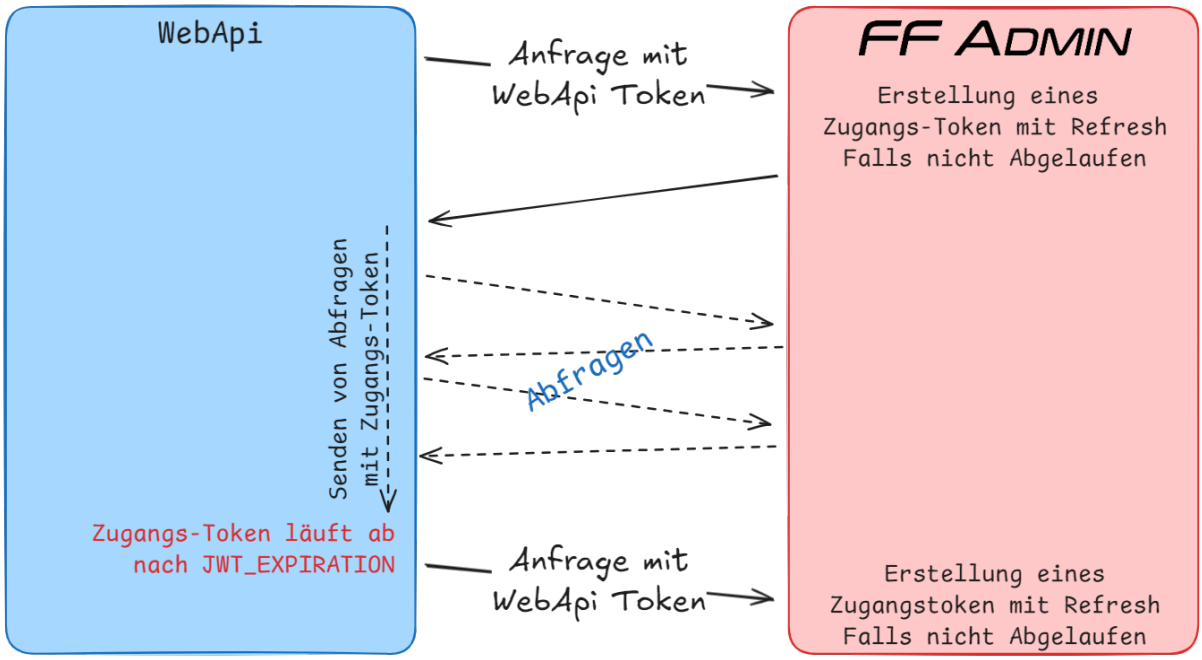
4.10.2 Berechtigungen



Einer WebApi können im Vergleich zu Benutzern nur direkte Berechtigungen zugewiesen werden (analog zu den Rollen).
Das Berechtigungsmodell unterscheidet zwischen Lese-, Erstellungs-, Änderungs- und Löschberechtigungen. Die Berechtigungen sind abgestuft. Das heißt, wer anlegen darf, darf auch lesen. Wer bearbeiten darf, darf auch anlegen und dementsprechend auch lesen usw.
Die Berechtigungen sind entsprechend der Bereiche in der Navigationsleiste gruppiert. Wenn die Berechtigung für einen Abschnitts auf Lesen gesetzt ist, kann der Benutzer mit dieser Berechtigung Daten in allen Modulen des Abschnitts lesen.
Erweiterte Berechtigungen können pro Modul gesetzt werden. Dabei gelten die Berechtigungen des Abschnitts immer mehr als die eines Moduls innerhalb des Abschnitts.

4.10.3 WebApi Zugriffsablauf

Die WebApi bezieht den Zugang wie folgt:



Zur einfacheren Verwendung der WebApi in eigenen Anwendungen kann das NPM-Paket `@ff-admin/webapi-client` verwendet werden.
Dieses ist unter https://code.jk-effects.cloud/FF-Admin/ff-admin-webapi-client verfügbar.

4.11 Anwendungsspezifische Einstellungen

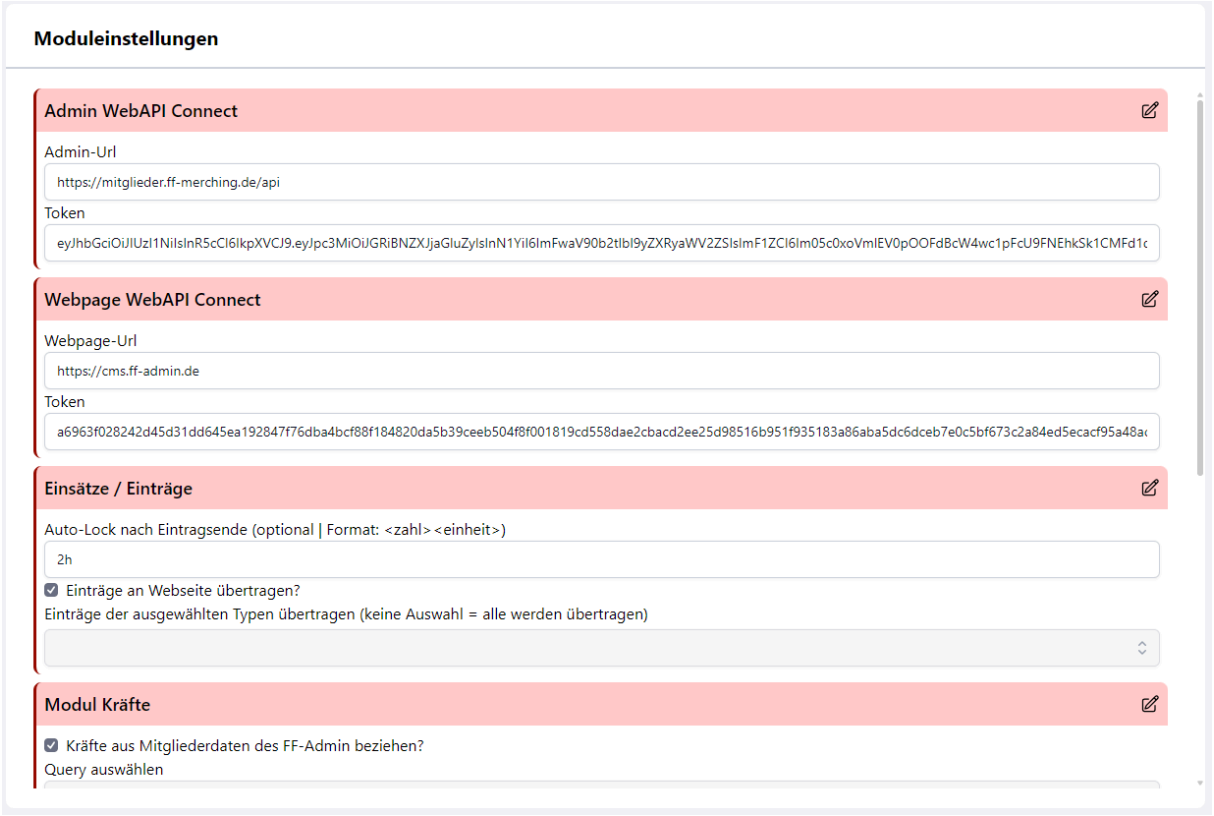
Das Modul Einstellungen ermöglicht eine flexible globale Konfiguration der Anwendung - ohne Neustart des Systems. Alle Anpassungen können direkt zur Laufzeit vorgenommen werden. Dadurch lassen sich beispielsweise Vereinslogos, Icons oder Texte im Login-Bereich individuell anpassen, ohne in den laufenden Betrieb einzugreifen.

Neben dem optischen Vereinsauftritt können auch grundlegende Informationen wie Links zum Impressum, zur Datenschutzerklärung oder zur Vereinswebseite hinterlegt werden. Diese Daten fließen dann automatisiert an verschiedenen Stellen im System ein.

Darüber hinaus ersetzt das Einstellungsmodul Teile der früheren, fest codierten Umgebungsvariablen (ENV). Werte wie etwa das Backup-Intervall oder E-Mail-Konten für den Versand können direkt in der Oberfläche geändert werden.

Insgesamt erlaubt das Modul eine Anpassung des Systems ohne Zugriff auf die Serverkonfiguration und Neustarts.

4.12 Modulspezifische Einstellungen



Das Modul Moduleinstellungen erweitert das bestehende Einstellungssystem um spezifische Optionen, die ausschließlich einzelne Module betreffen. Beispielsweise kann festgelegt werden, wie lange nach einem Eintrag diese automatisch gesperrt oder ob und welche Daten aus FF Admin Synchronisiert werden sollen.

Mit den Moduleinstellungen lassen sich Funktionen und Darstellungen einzelner Module gezielt steuern, ohne das Gesamtsystem zu beeinflussen.

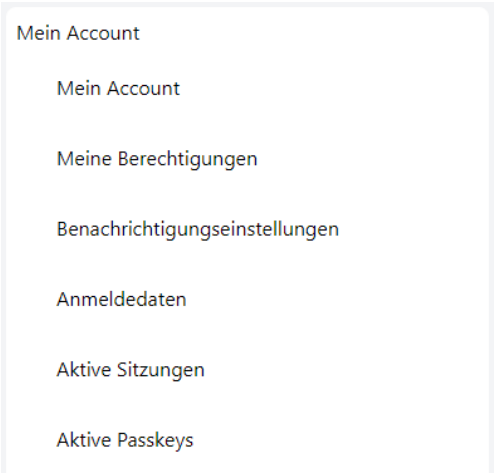
Admin WebAPI Connect: Damit Daten aus FF Admin synchronisiert werden können, muss ein WebAPI Token aus dem Admin angegeben werden. Die URL ist nur die URL, unter der das Backend läuft. Ein angegebener Pfad wird ignoriert. Bei der Speicherung der Einstellung wird direkt die Gültigkeit geprüft.
Webpage WebAPI Connect: Damit Daten zu FF Wbpage synchronisiert werden können, muss ein WebAPI Token aus dem CMS angegeben werden. Die URL ist die, die zum aufrufen der CMS-Ansicht verwendet wird. Ein angegebener Pfad wird ignoriert.
Auto-Lock: Einträge können automatisch auf gesperrt gesetzt werden, wenn eine Bestimmte Dauer seit dem gesetzten Ende des Eintrags vergangen ist. Die Dauer kann x Stunden, Tage,

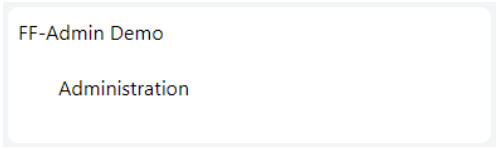
Wochen, Monate oder Jahre betragen. Der Job zum Sperren läuft alle 30 Minuten. Dadurch kann sich das Sperren um 30 min verzögern.

Synchronisierung: Die Datensynchronisierung aus dem Admin muss gezielt für verfügbare Module aktiviert werden. Ist die Synchronisierung aktiviert, kann in den Einstellungen gestartet werden. Die Synchronisierung läuft immer nachts um 0Uhr.

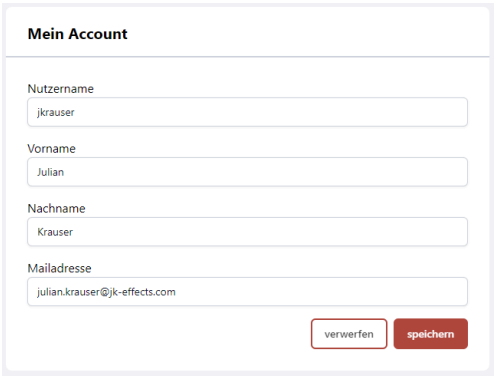
5 Benutzerbereich und Accounteigenschaften

Der Accountbereich ist für jeden Benutzer durchgehend zugänglich und gliedert sich in allgemeine Kontoinformationen sowie einen Administrations- bzw. Eigentümerbereich.





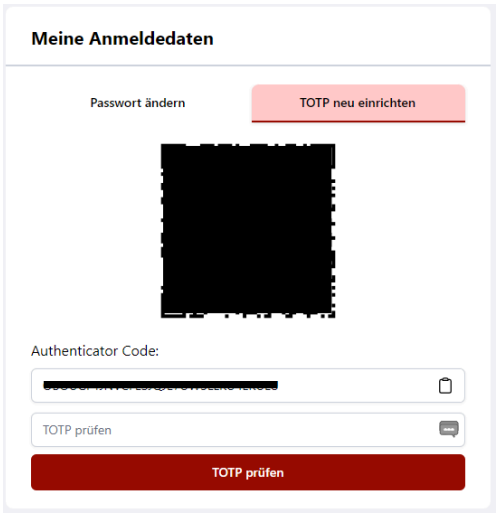
5.1 Zugang und Anmeldedaten

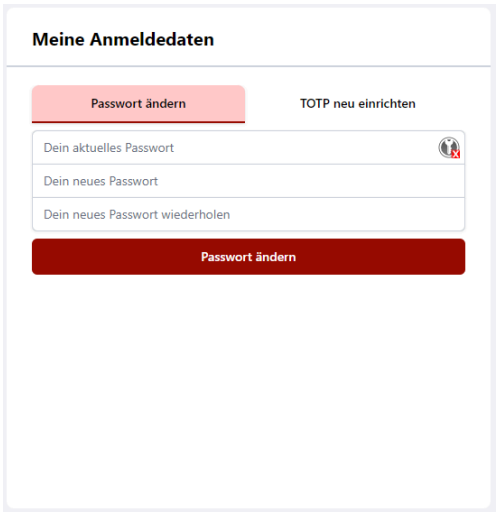


Die Kontoinformationen sind in zwei separate Bereiche unterteilt: Der Bereich **Mein Account** zeigt allgemeine Accountdaten wie Benutzername und E-Mail-Adresse an, die auch von einem Administrator direkt in der App bearbeitet werden können. Im Bereich **Anmeldedaten** können die Einstellungen für die Authentifizierung verwaltet werden - entweder das zeitbasierte Einmalpasswort (TOTP) oder das klassische Passwort.

Nutzer können sich entweder mit einem zeitbasierten Einmalpasswort (TOTP) oder einem klassischen Passwort anmelden. Je nach gewählter Methode stehen folgende Optionen zur Verfügung:

- **TOTP-Anmeldung:** Der TOTP-QR-Code kann erneut angezeigt werden, um die Authentifizierung auf einem weiteren Gerät einzurichten. Alternativ kann zu einer Passwort-basierten Anmeldung gewechselt werden.
- **Passwort-Anmeldung:** Das Passwort kann geändert oder zu einer TOTP-basierten Anmeldung gewechselt werden.
- **Passkey-Anmeldung:** Passkeys können als alternative Loginmethode erstellt werden und erleichtern den Login. Passkeys ersetzen allerdings nicht das gesetzte Passwort bzw. das eingerichtete TOTP. (Abschnitt 5.4)





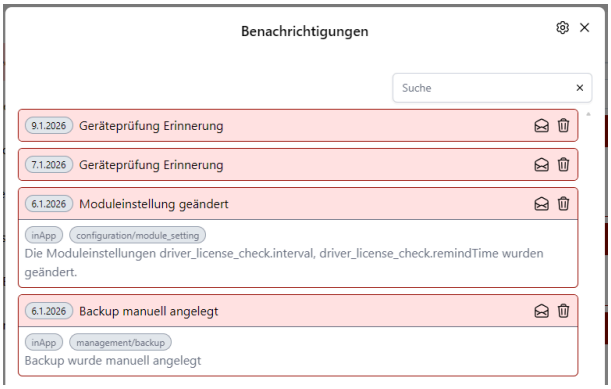
5.2 Benachrichtigungen

Benutzer können Benachrichtigungen zu Vorgängen der Anwendung einstellen und erhalten. Benachrichtigungen werden immer gespeichert und können über die Glocke in der Navigationsleiste angezeigt werden.
Für die Module, welche Benachrichtigungen versenden, kann der Versandweg eingestellt werden. Zur Verfügung stehen aktuell:

- **In-App**: Nachrichten werden direkt in der Anwendung angezeigt, wenn diese geöffnet ist
- **E-Mail**: Benachrichtigungen werden per E-Mail versendet
- **Web-Push**: Geplant für zukünftige Versionen, aber schon einstellbar.

Einstellungen zu den Benachrichtigungen können nur für Module vorgenommen werden, auf die der Account Zugriff hat.

5.2.1 Benachrichtigungsanzeige



In der Benachrichtigungsanzeige werden alle Benachrichtigungen zentral aufgelistet. Für jede Benachrichtigung sind folgende Informationen ersichtlich:

- Der Nachrichteninhalt
- Das sendende Modul
- Die verwendeten Zustellwege (In-App, E-Mail, Web-Push)

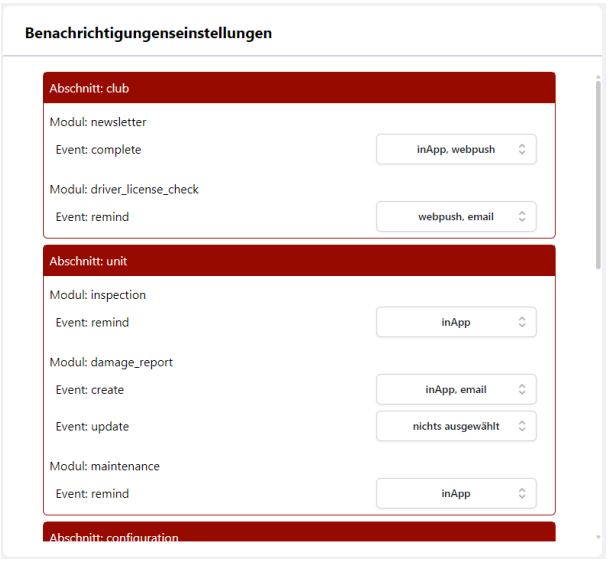
Hier können versendete Benachrichtigungen jederzeit nachgelesen werden.

5.2.2 Benachrichtigungseinstellungen

Die Benachrichtigungseinstellungen sind über das Zahnrad in der Nachrichtenanzeige oder im Usermenü unter „Mein Account“ erreichbar.
Für jedes Modul und Event können die Versandwege individuell konfiguriert werden:

- **In-App**: Direkte Anzeige in der Anwendung
- **E-Mail**: Versand per E-Mail
- **Web-Push**: Versand per Push-Benachrichtigung (geplant)

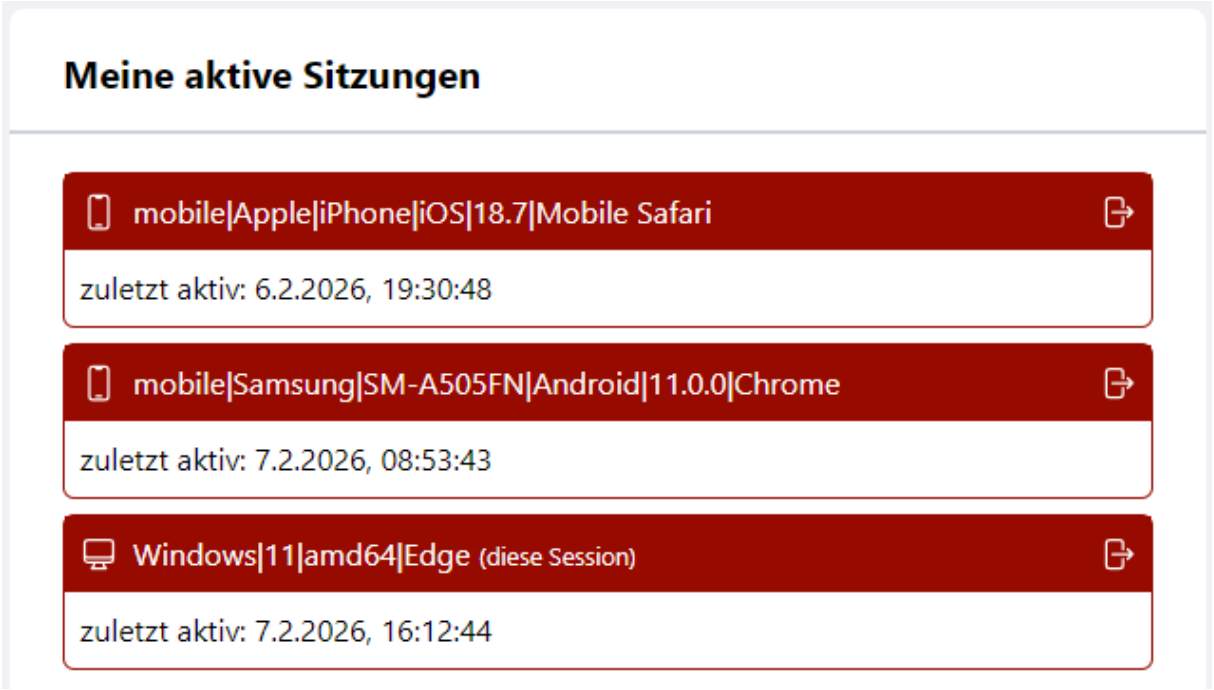
Es können mehrere Versandarten gleichzeitig aktiviert werden.



Benachrichtigungen werden für folgende Ereignisse versendet:

- **create**: Neues Element wurde erstellt
- **update**: Element wurde aktualisiert
- **delete**: Element wurde gelöscht
- **complete**: Vorgang wurde abgeschlossen (Bsp.: Newsletter wurde fertig versandt)
- **remind**: Erinnerung an anstehende Aufgabe (Bsp.: Prüfung ist fällig)

5.3 Sessionverwaltung



Die Sessionverwaltung bietet Nutzern umfassende Kontrolle über ihre aktiven Anmeldungen. Mit dieser Funktion können Sie jederzeit einsehen, auf welchen Geräten Ihr Account derzeit aktiv ist und Details zu den entsprechenden Sitzungen abrufen.

5.3.1 Geräteerkennung und Datenschutz

Bei jeder Anmeldung erfasst das System automatisch Geräteinformationen wie Betriebssystem, Browser und Gerätetyp. Diese Daten werden direkt vom Gerät bereitgestellt und ermöglichen eine zuverlässige Geräteidentifikation – ohne dabei Fingerprinting-Techniken zur vollständigen Geräteprofilierung einzusetzen.

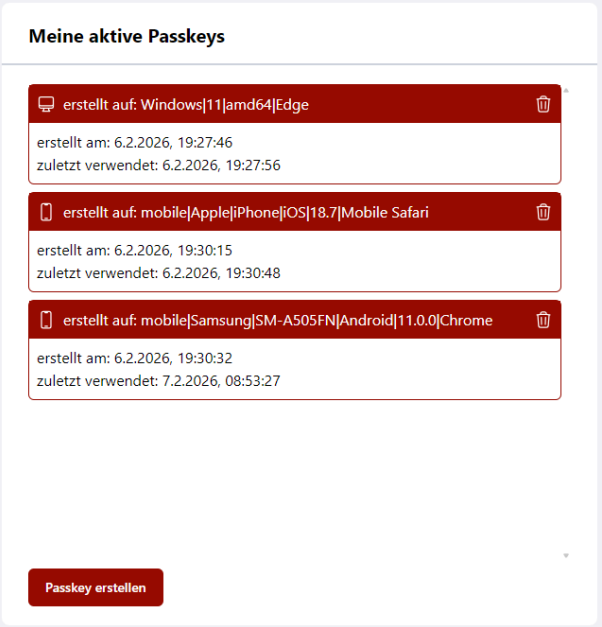
5.3.2 Verwaltung aktiver Sessions

Sie haben die Möglichkeit, Sessions von anderen Geräten aus zu beenden:

- **Ist die App aktiv:** Das betroffene Gerät wird sofort abgemeldet.
- **App ist inaktiv:** Der Zugriff wird beim nächsten Öffnen der Anwendung blockiert - eine erneute Anmeldung ist erforderlich.

Diese Funktion erhöht die Sicherheit Ihres Accounts und gibt Ihnen vollständige Kontrolle über Ihre aktiven Sitzungen.

5.4 Passkeys



Passkeys sind eine sichere Alternative zu Passwörtern. Sie basieren auf der FIDO2-Technologie und ermöglichen es einem Nutzer, sich mit biometrischen Daten (Fingerabdruck, Gesichtserkennung) oder einer PIN zu authentifizieren, ohne sich ein komplexes Passwort merken zu müssen.
Die Passkeys werden direkt auf dem Gerät gespeichert und ersetzen klassische Zugangsdaten komplett. Beim Login erkennt die Anwendung automatisch, dass ein Passkey vorhanden ist, und bietet diese Option direkt an - dadurch muss sich ein Nutzer nicht mehr an Passwörter erinnern.

Vorteile von Passkeys

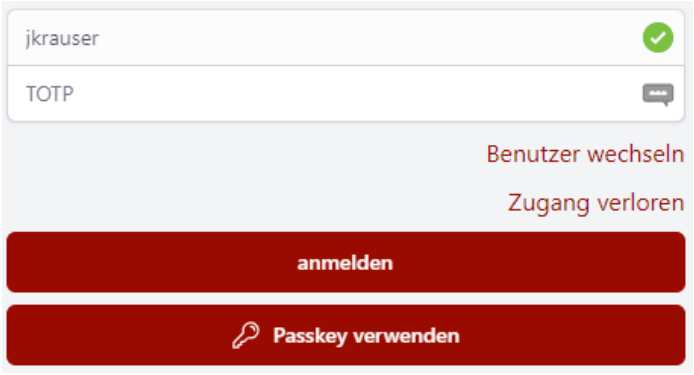
- **Einfacherer Login**: Statt Passwort eingeben reicht Fingerabdruck oder Gesichtserkennung
- **Höhere Sicherheit**: Passkeys sind resistent gegen Phishing und Brute-Force-Attacken
- **Gerätübergreifend**: Dein Passkey wird auf mehreren Geräten synchronisiert und kann auch auf anderen Geräten verwendet werden

5.4.1 Erstellung eines Passkeys

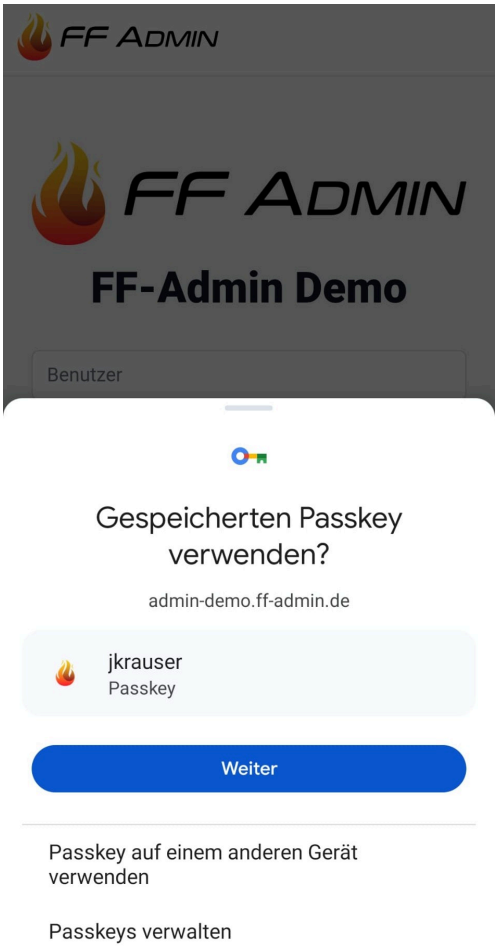
Ein Passkey kann nur erstellt werden, wenn der Nutzer bereits angemeldet ist. In den Kontoeinstellungen unter `Meine aktiven Passkeys` lässt sich ein neuer Passkey hinzufügen.
Nach Klick auf `Passkey erstellen` führt das Gerät durch den Erstellungsprozess und fordert zur Bestätigung eine PIN oder biometrische Authentifizierung an.
Passkeys können auch über ein anderes Gerät erstellt werden. Nach Auswahl dieser Option wird ein QR-Code angezeigt, den man mit einem anderen Gerät scannen kann. Dadurch werden beide Geräte synchronisiert und der Passkey steht auf beiden zur Verfügung.

5.4.2 Login mit Passkeys

Passkeys können auf dem Gerät direkt nach der Erstellung verwendet werden. Ist der Nutzername schon Hinterlegt, wird ein Knopf unterhalb des Login-Formulars angezeigt:



Sollte noch kein Nutzername eingegeben sein, wird ein vorhandener Passkey zur Auswahl angezeigt, wenn ins Feld „Benutzername“ geklickt wird.
Bei Auswahl eines Passkeys erfolgt eine Bestätigung durch den Nutzer. Alternativ kann ein anderes Gerät zum Login verwendet werden: Nach Auswahl dieser Option wird ein QR-Code angezeigt, über den die Anmeldung auf einem anderen Gerät erfolgen kann.



5.5 Übertragung Administration

Bei der Übertragung der Administration wird ein anderer Nutzer zum Owner ernannt und erhält damit Vollzugriff auf die gesamte Anwendung, unabhängig von einzelnen Berechtigungen.
Der bisherige Administrator verfügt danach nur noch über die Berechtigungen, die ihm durch seine Rollen oder direkten Zuweisungen zuteil werden.

6 Ökosystem FF Admin

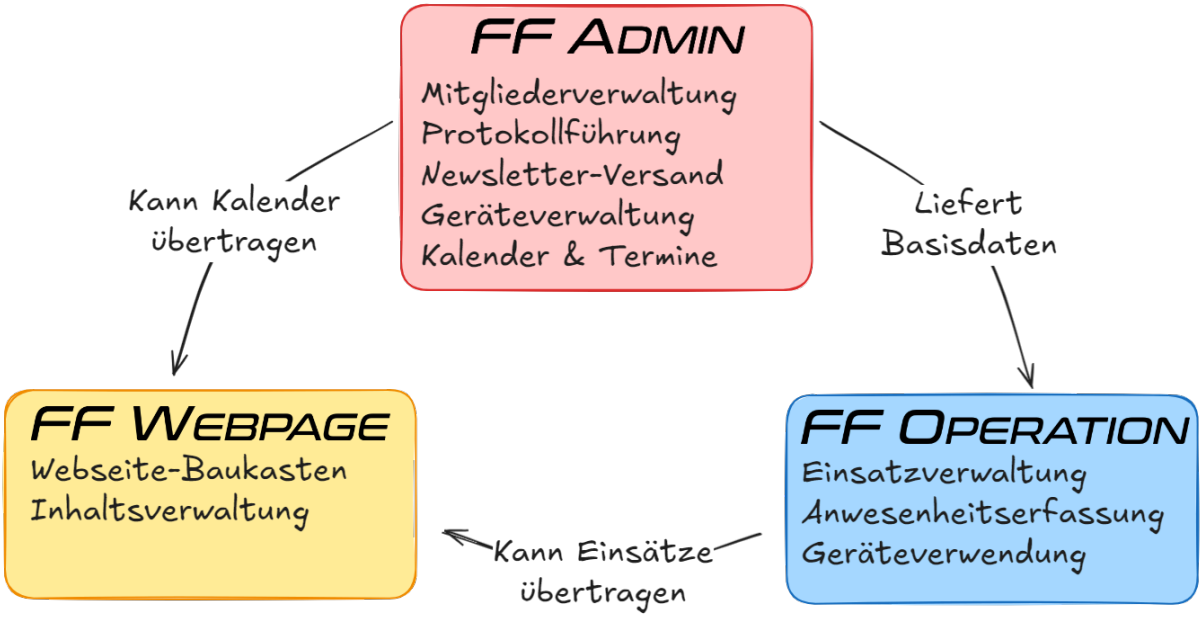


Abbildung 61: Übersicht zum Ökosystem

Das **FF Ökosystem** bietet eine zentrale Lösung für die Verwaltung von Mitgliedern, Einsätzen und Inhalten.

FF Admin ist das Herzstück mit der Mitglieder- und Geräteverwaltung sowie der Module zur Wehr- und Vereinsverwaltung. Es stellt Stammdaten bereit und ermöglicht mit allen seinen Modulen die effiziente Verwaltung einer Feuerwehr oder Vereins.

FF-Webpage erleichtert die Erstellung und Verwaltung von Webseiteninhalten. Kalender- bzw. Einsatzdaten können von FF Admin und FF Operation an die Webseite geschickt und dort veröffentlichen werden, um Mitglieder und die Öffentlichkeit auf dem Laufenden zu halten.

FF Operation unterstützt das Einsatzmanagement, die Anwesenheitserfassung und den Geräteeinsatz. Es kann die Mitgliederdaten, Gerätschaften und co aus FF Admin beziehen.

7 Roadmap

Folgende Funktionalitäten sind für FF Operation in Planung (Auszug):

- **Schnittstellen:** Implementierung von Schnittstellen wie UCRI, WDX3...
- **Dynamische Formulare:** Einstellbare Anzeige von Feldern je nach Eintragsart
- **Protokollierung:** Erstellen von unveränderbaren Einträgen zu Entscheidungen... ohne Möglichkeit zur Änderung.
- **Statistik:** Statistische Auswertung der Einträge nach Uhrzeiten, Häufigkeiten, Anwesenheiten...

Eine ausführliche Liste geplanter Funktionen kann im Git unter Issues gefunden werden:
https://code.jk-effects.cloud/FF-Admin/ff-operation/issues
https://code.jk-effects.cloud/FF-Admin/ff-operation-server/issues