Einstellungen und Benutzerverwaltung

Einstellungen und Benutzerverwaltung

Dieses Kapitel bündelt die beiden Mandanten-Bereiche, in denen Sie die Konfiguration Ihrer Instanz verwalten: die **Einstellungen** und die **Benutzerverwaltung**.

Einstellungen

Die Seite **Einstellungen** ist Ihre zentrale Schalt-Anlage. Sie erreichen sie über die Hauptnavigation.

Alarmdienste verwalten

Die wichtigste Kachel. Öffnet ein Modal mit allen DIVERA-bezogenen Einstellungen. Diese wurden bereits im Kapitel „DIVERA24/7-Integration" behandelt. Nochmal die Kurzfassung der Toggles:

Einstellung	Zweck
DIVERA24/7 Auth-Key	API-Schlüssel für Outbound-Calls
DIVERA24/7 Inbound	Eingehende Webhooks verarbeiten (ja/nein)
DIVERA24/7 Outbound	Status-Rückmeldungen an DIVERA senden (ja/nein)
Mandown an DIVERA	Mandown-Ereignisse (cmd 0A) als Einsatz in DIVERA erzeugen
Notrufe an DIVERA	Notruf-Ereignisse (cmd 08) als Einsatz in DIVERA erzeugen
Tear-Off Alarme weiterleiten	Tear-Off-Ereignisse (cmd 0B) als Einsatz erzeugen

Änderungen werden sofort aktiv – kein Neustart notwendig.

Pager automatisch registrieren

Ein Toggle in den System-Einstellungen. Wenn aktiviert, dürfen sich **MQTT-Pager ohne Vorregistrierung** einfach verbinden. Der Broker legt dann automatisch einen Pager-Eintrag in der Datenbank an und ordnet ihn Ihrem Mandanten zu.

Das Flag greift **nur für MQTT**. TCP-Pager müssen immer vorregistriert sein, weil bei TCP die Mandantenzuordnung nicht zuverlässig abgeleitet werden kann.

Wann aktivieren?

- Während der initialen Einrichtung, wenn Sie viele MQTT-Pager auf einmal ausrollen.
- Wenn Ihre MQTT-Pager zuverlässig mit der richtigen Broker-URL konfiguriert sind.

Wann deaktivieren?

- Im Regelbetrieb. Neue Pager sollen dann bewusst über die Pager-Seite angelegt werden, nicht automatisch.
- Sicherheitsbedenken: Ein Angreifer mit gültiger Tenant-URL könnte sonst unerwünschte Pager registrieren (zwar harmlos, aber nicht ideal).

Pager-Inaktivität (Minuten)

Schwellwert, ab wann ein Pager als „inaktiv" / „offline" gilt. Default: **30 Minuten**. Wenn Ihr Pager häufiger Keep-Alives sendet (z.B. alle 60 Sekunden), können Sie den Wert reduzieren. Wenn Ihre Pager seltener senden (z.B. nur alle 10 Minuten), erhöhen Sie ihn.

Achtung: Das hier eingestellte Intervall gilt für Anzeigen in GUI. Das interne „Versand nur wenn online"-Verhalten nutzt immer feste 15 Minuten.

E-Mail-Einstellungen (Mailgun)

Damit Passwort-Reset-Mails und Einladungs-Mails versendet werden können, müssen Sie einen SMTP-fähigen Service hinterlegen. Der Broker nutzt Mailgun.

Einzutragen:

- **Mailgun API-Key** – aus Ihrem Mailgun-Account
- **Mailgun Domain** – die in Mailgun verifizierte Domain (z.B. `mail.mustermann-fw.de`)
- **Absender-Name** – z.B. „Feuerwehr Musterstadt"
- **Absender-E-Mail** – z.B. `noreply@mustermann-fw.de`

Nach dem Speichern können Sie einen **Test-Mail** versenden, um die Konfiguration zu prüfen.

System-Status-Einstellungen

Unter **System** können Sie Schwellwerte für das Dashboard-Ampel-System anpassen:

- Wie viele Stunden ohne Alarm-Empfang sollen rot markiert werden?
- Wann soll der „System gesund"-Indikator auf Warnung wechseln?

Diese Einstellungen sind meist ohne Anpassung sinnvoll konfiguriert.

Benutzerverwaltung

Die Seite **Benutzerverwaltung** listet alle Benutzer Ihres Mandanten und ermöglicht Anlegen, Bearbeiten und Löschen.

Benutzerrollen

Der Broker kennt für Mandanten-Ebene zwei Rollen:

`admin`
Vollzugriff auf alle Funktionen des Mandanten. Kann weitere Benutzer anlegen, Pager bearbeiten, Einstellungen ändern.

`user`
Lesender Zugriff. Kann Dashboard, Logs, Alarme sehen, aber nichts ändern. Nützlich für Personal, das nur informativ zugreifen soll (z.B. Fahrzeugführer, die über das Dashboard Ihre Alarme einsehen).

Eine Rolle **`super_admin`** **existiert**, ist aber nicht auf Mandanten-Ebene sichtbar. Super-Admins haben keinen Mandanten-Bezug.

Neuen Benutzer anlegen

Klicken Sie auf **Neuen Benutzer anlegen**. Geben Sie an:

- E-Mail (muss eindeutig sein)
- Initial-Passwort (der Benutzer wird aufgefordert, es beim ersten Login zu ändern)
- Rolle (**`admin`** oder **`user`**)
- Vorname, Nachname (optional)

Nach Anlage wird – wenn Mailgun konfiguriert ist – eine Einladungs-Mail versendet.

Benutzer bearbeiten

Klick auf einen Benutzer öffnet die Detail-Ansicht. Änderbar sind: Name, Rolle, aktiv/inaktiv.

Aktiv/Inaktiv ist nützlich, um einen Benutzer temporär zu sperren, ohne ihn zu löschen – z.B. bei Urlaub. Ein inaktiver Benutzer kann sich nicht einloggen, bleibt aber in der Datenbank und kann alle historischen Aktionen nachvollziehen.

Passwort zurücksetzen

Für jeden Benutzer gibt es einen Button **Passwort zurücksetzen**. Das System sendet dem Benutzer eine Reset-Mail (Mailgun notwendig). Alternativ können Sie ein neues Passwort manuell vergeben.

Benutzer löschen

Löschen entfernt den Benutzer dauerhaft aus der Datenbank. **Historische Einträge** (z.B. „Alarm gesendet von X") bleiben erhalten, zeigen aber keinen klickbaren Benutzer-Link mehr.

Eine gängige Alternative: Benutzer auf **inaktiv** setzen statt löschen. Das bewahrt die Audit-Spur.

Die Super-Admin-Beziehung

Manchmal haben Super-Admins Ihnen temporär Zugriff auf Ihre Mandanten-Instanz gegeben, um zu helfen. Der Super-Admin kann sich dafür **als Sie einloggen** – über einen Login-Token, der in seinem Admin-Panel erzeugt wird.

Sie sehen solche Einloggungen im Audit-Log. Wenn Sie sich unsicher sind, fragen Sie Ihren Super-Admin.

Passwort-Richtlinien

Die Plattform erzwingt keine harten Passwort-Regeln (Mindestlänge, Sonderzeichen), sondern empfiehlt starke Passwörter. Als Orientierung:

- mindestens 12 Zeichen
- Mischung aus Groß-/Kleinbuchstaben, Ziffern, Symbolen
- keine Wörterbuch-Wörter
- keine persönlichen Daten (Namen, Geburtstage)

Administratoren sollten zusätzlich einen **2. Faktor** nutzen, sofern der Browser bzw. das Gerät 2FA unterstützt. Die Plattform selbst bietet aktuell kein eingebautes 2FA – das ist für zukünftige Versionen geplant.

Audit und Nachvollziehbarkeit

Alle Änderungen in Einstellungen und Benutzerverwaltung werden in `system_logs` mit der Kategorie `audit` protokolliert. Super-Admins können diese Protokolle im Admin-Panel einsehen.

Mandanten-Admins sehen Audit-Einträge in ihrer eigenen **Logs**-Seite unter der Ansicht „System".