

Inhaltsverzeichnis

Benutzerverwaltung

Warum?

Voraussetzungen

Konfiguration in sw2

Allgemein

Benutzer

Gruppen

Rollen

Typische Anwendungsfälle

Einstellungen mit Kennwort sichern

Benutzerverwaltung WEG mit Ladepunkten

2

2

2

2

3

3

5

7

9

9

9



Benutzerverwaltung

Warum?

Das openWB-System ist ein vollwertiger Energiemanager, der kontinuierlich mit den Ideen unserer Nutzer:innen und unseres Teams weiterentwickelt wird.

Dank der modularen Struktur der software2 (sw2) ist es möglich, nicht nur Privathaushalte, sondern zunehmend auch **größere Installationen wie Ladeparks, Mehrfamilienhäuser sowie WEG/Mieterstrom-Modelle** abzudecken [EMS in MPH](#).

Das alles mit einer einzigen open source Lösung, die weitgehende Unabhängigkeit, eine hohe Flexibilität bei keinen bis sehr geringen laufenden Kosten bietet. Unsere Philosophie lautet „**1x openWB-Hardware kaufen und mitmachen!**“.

Die ab 2.2.0 integrierte **Benutzerverwaltung (BV)** ermöglicht:

- die teils umfangreichen EMS- und LM-Konfigurationen per Passwort zu schützen (Manipulationsschutz)
- benutzerdefinierten Zugriff mittels frei konfigurierbarem Rechtesystem → eingeschränkte Anzeigen, Bedienung, usw.
- Zwei-Faktor-Authentifizierung beim Fernzugriff über die openWB Cloud (einmal die Cloud-Daten zum Aufbau der Verbindung und dann individuelle Nutzerdaten zum Zugriff auf das System)

Voraussetzungen

Aus Sicherheitsgründen ist die Abschaltung unverschlüsselter Datenübertragung (<http://...>) erforderlich.

Konfiguration in sw2

Allgemein

Die Konfiguration der BV erfolgt unter *Einstellungen* → *System* → *Sicherheit*.

• Aktivierung der BV

- Die Benutzerverwaltung wird auf **An** gestellt und im Anschluß ist ein „softer“ **Neustart** erforderlich unter *Einstellungen* → *System* → *System* → *Ja* → *Betrieb* → *Neustart*. Der Reboot-Vorgang kann bis zu 10 min dauern.
- Der Standard-Zugang lautet: Benutzername „**admin**“, Passwort „**openwb**“
- Das Passwort ist dringend nach der ersten Aktivierung **auf ein individuelles PW zu ändern!**
- Des Weiteren ist **eine eigene E-Mail-Adresse festzulegen**, um im Zweifel die **Passwort vergessen**-Funktion nutzen zu können!
- Der Nutzer **admin** kann nicht gelöscht werden!
- Die Rollen von **admin** können nicht verändert werden (Schutz vor Aussperren).

• De-Aktivierung und Zurücksetzen der BV

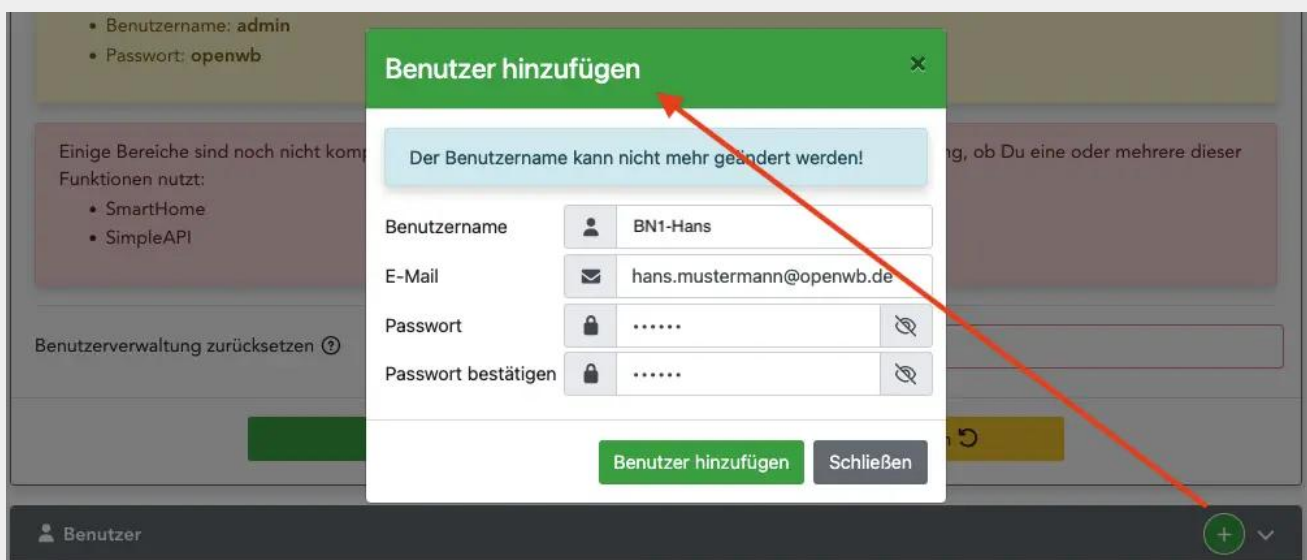
- Die Benutzerverwaltung wird auf **Aus** gestellt und im Anschluß ist ein „softer“ **Neustart** erforderlich unter *Einstellungen* → *System* → *System* → *Ja* → *Betrieb* → *Neustart*. Der Reboot-Vorgang kann bis zu 10 min dauern.
- Nach dem Reboot kann die BV über den Button **Zurücksetzen** in den Startzustand versetzt werden (→ **Entfernen aller Benutzer und Gruppen**).

Benutzer

Die Konfiguration der **Benutzer** erfolgt unter *Einstellungen* → *System* → *Sicherheit*.



- Einige Benutzer werden **automatisch** vom System angelegt. Diese Benutzer können mit weiteren Rechten durch **zusätzliche Gruppen/Rollen** angepasst werden.
 - Benutzer: **Display-Intern**
 1. wird von einem integrierten Display dieser openWB verwendet
 2. wird unabhängig davon angelegt, ob das Display aktiviert ist oder nicht
 3. Gruppe „display“ wird automatisch zugeordnet
 - Benutzer: **Display-<eine IP>**
 1. wird für jede eingerichtete secondary-openWB automatisch angelegt (bei openWB-DUO's nur einmalig)
 2. Gruppe „display“ wird automatisch zugeordnet
- **neue Benutzer** anlegen → mit „+“ im Kopf der aufgeklappten Karte **Benutzer** analog zu Ladepunkten, Fahrzeugen etc.



Hinweise

Der Name des Benutzers kann später nicht mehr geändert werden!
 Die Groß-/Kleinschreibung ist wichtig! -> "Hans" ist nicht gleich "hans"!
 Die zugehörige E-Mail wird benötigt, um ein vergessenes Kennwort zurückzusetzen!

- **Benutzer-Karte**
 - Im Kopf einer Benutzer-Karte wird angezeigt, ob der Benutzer „**Aktiv**“ ist. Durch Klick auf **Aktiv** kann der Benutzer deaktiviert werden (und vice versa).
 - Deaktivierte Benutzer haben keinen Zugriff mehr. → praktisch für temporäre Sperren, ohne später alle Rollen/Gruppen wieder neu zuweisen zu müssen
 - Das Symbol vor dem Namen ist bei deaktivierten Benutzern durchgestrichen.
 - Wird die Karte eines Benutzers aufgeklappt, werden zwei Aktionen sichtbar: **de-aktivieren** und **löschen**

- Feld „Zusatzinformationen“: beliebiger Freitext zur individuellen Kennzeichnung eingebbar
- Rechte werden über **Gruppen** und/oder **Rollen** zugewiesen.

The screenshot shows the 'Benutzer' (User) management interface. The header bar has a red arrow pointing to the 'Benutzer' label. Below the header, the user 'BN1-Hans' is selected, and a green arrow points to the 'Aktiv' status button. The form contains the following fields:

- Benutzername:** BN1-Hans
- E-Mail:** hans.mustermann@openwb.de
- Passwort:** (masked)
- Zugewiesene Gruppen:** Wohnung1
- Zugewiesene Rollen:** (empty)
- Zusatzinformationen:** Mieter der Wohnung1

A green 'Speichern' button is located at the bottom of the form.

Gruppen

Die Konfiguration der **Gruppen** erfolgt unter *Einstellungen* → *System* → *Sicherheit*.

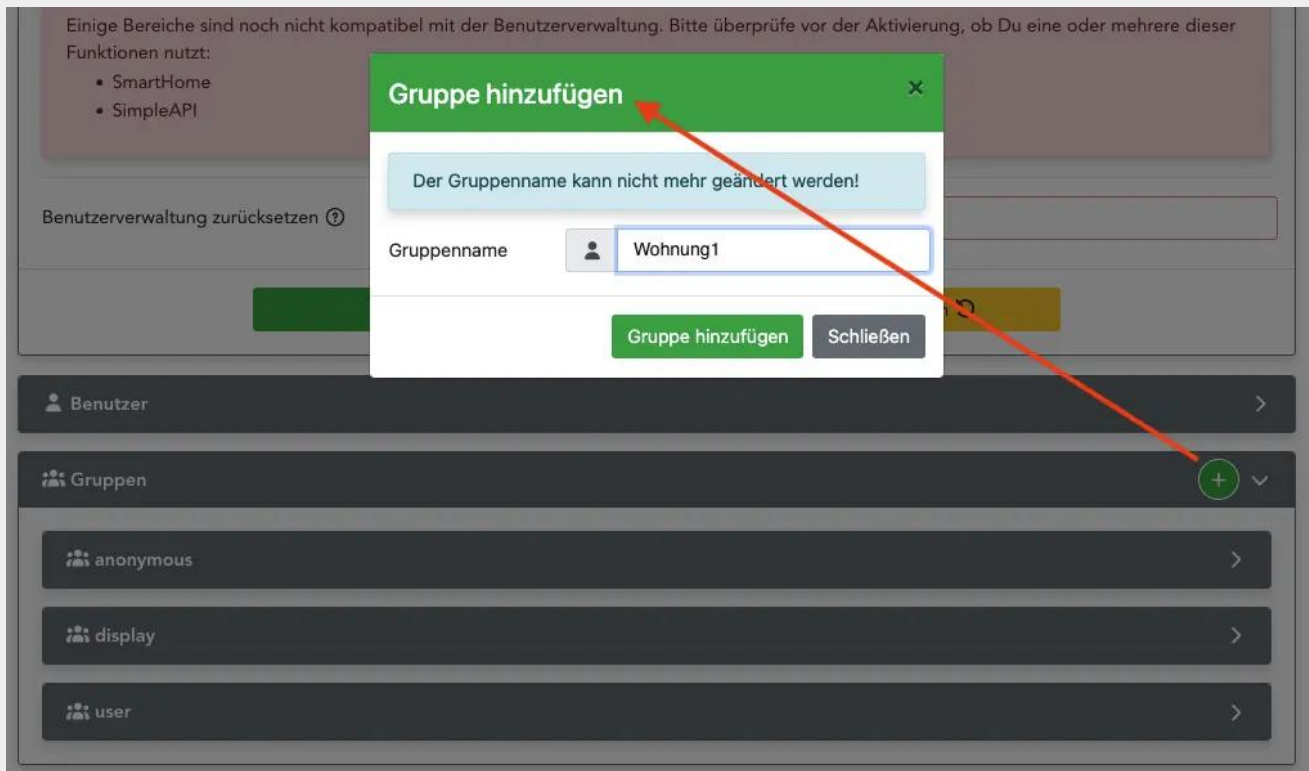
The screenshot shows the 'Gruppen' (Groups) management interface. The header bar has a red arrow pointing to the 'Gruppen' label. Below the header, a list of groups is shown:

- anonymous
- display
- user

A red arrow points to the 'Add' (+) button in the top right corner of the header.

- Einige Gruppen sind bereits **vordefiniert** vom System angelegt. Diese System-Gruppen haben fest vordefinierte Rollen und **können nicht angepasst/gelöscht** werden.
 - Gruppe: **anonymous**
 1. regelt alle anonymen Zugriffe ohne Anmeldung
 2. Die zugewiesenen Rollen sind fix und können nicht bearbeitet werden.
 - Gruppe: **display**
 1. stellt lesend grundlegende Systeminfos und Einstellungen bereit, welche für Display-Themes benötigt werden
 2. gibt keinen Zugriff auf Daten frei (Display ist „leer“, Datenzugriff über eigene Gruppe oder direkt bei den Display-Benutzern)
 3. Die zugewiesenen Rollen sind fix und können nicht bearbeitet werden.
 - Gruppe: **user**
 1. Basis für individuelle Benutzer, um auf (Display-)Themes zuzugreifen

2. gibt keinen Zugriff auf Daten frei (Display/Theme ist „leer“)
 3. Die zugewiesenen Rollen sind fix und können nicht bearbeitet werden.
- **neue Gruppe** anlegen → mit „+“ im Kopf der aufgeklappten Karte **Gruppen** analog zu Ladepunkten, Fahrzeugen etc.



Hinweise

Eigene Gruppen sind sinnvoll, wenn mehrere Benutzer identische Rechte bekommen sollen.

Auch bei nur einem Benutzer ist es sinnvoll, falls später weitere Benutzer hinzukommen.

Der Name der Gruppe kann später nicht mehr geändert werden!

- **Gruppen-Karte**
 - Rechts im Kopf der Karte kann eine Gruppe gelöscht werden (nicht System-Gruppen).
 - Feld „Beschreibung“: beliebiger Freitext
 - Feld „Zusatzinformationen“: beliebiger Freitext
 - Feld „Zugewiesene Benutzer“: Auswahlliste aller vorhandenen Benutzern - frei zuordnbar
 - Feld „Zugewiesene Rollen“: Auswahlliste aller vorhandenen Rollen - frei zuordnbar

Gruppen

Wohnung1

Gruppenname: Wohnung1

Beschreibung: Wohnung1 im EG links (Mietwohnung)

Zugewiesene Benutzer: BN1-Hans

Zugewiesene Rollen:

- Basisdaten: Hauptseite/Theme
- Basisdaten: Benutzer
- Daten: Ladepunkt 'MQTT-Ladepunkt 1' (3) lesen und bedienen
- Daten: Ladepunkt Summendaten lesen
- Daten: Verlaufdiagramm lesen
- Daten: Fahrzeug 'BMW i3 (Hans)' (1) lesen und bedienen

Zusatzinformationen: Gruppe Wohnung1 bei Mieterwechsel nur den neuen Mieter zuweisen

Speichern ✓

Rollen

Die Konfiguration der **Rollen** erfolgt unter *Einstellungen* → *System* → *Sicherheit*.

Rollen

Rollen definieren die Zugriffsrechte (Access Control Lists, ACLs) für Benutzer und Gruppen. Jeder Benutzer oder jede Gruppe kann mehrere Rollen zugewiesen bekommen, wodurch sich die effektiven Zugriffsrechte zusammensetzen. openWB erstellt automatisch relevante Rollen während der Installation und bei der Aktivierung bestimmter Funktionen oder Bearbeitung von Ladepunkten, Geräten und Komponenten etc. Rollen können hier nicht bearbeitet oder gelöscht werden.

Versionsnummer der Rollendefinitionen: 3

Standard-Zugriffsrechte:

- <alle Topics> -> Veröffentlichen verboten
- <alle Topics> -> Empfangen verboten

Hier werden die Standard Zugriffsrechte (Access Control Lists, ACLs) angezeigt. Diese werden verwendet, wenn keine spezifischen ACLs für einen Benutzer oder eine Gruppe definiert sind oder die Topics nicht explizit abgedeckt werden.

lange weiterführende Rollenliste

- Basisdaten: Benutzer
- Basisdaten: Display
- Basisdaten: Hauptseite/Theme
- Basisdaten: System
- Daten: Externe Anwendungen lesen und schreiben

- Dieser Bereich ist **eher für Spezialisten** interessant, welche **direkt mit dem Broker** Daten austauschen wollen. Hier kann für **jede Rolle** eingesehen werden, welche Topics les-/schreibbar freigegeben werden.
- Die **Rollen sind fest vorgegeben**. Es können keine eigene Rollen angelegt werden und auch keine individuelle Rollen konfiguriert werden (aktuell noch kein Anwendungsfall bekannt).
- Normale Anwender sollten mit den **Rollen-Bezeichnungen** zurechtkommen. Als Zusatzinformation gibt es neben der Bezeichnung noch eine **Beschreibung** sowie ggf. einen blauen Infokasten in der Rollen-Karte. Der Infokasten kann jedoch nicht bei den einzelnen Komponenten, Ladepunkten, Fahrzeugen etc. verwendet werden (Einschränkung Broker-Schnittstelle).
- Zusatzinformationen:
 - Feld **Versionsnummer**: für den Anwender eigentlich nicht relevant, aber ggf. zur Fehlersuche wichtig, wird eventuell durch Updates hochgezählt
 - Feld **Standard-Zugriffsrechte**: nur informativ, hat für den Anwender keine Relevanz, ggf. für die Spezialisten interessant

Schema der Bezeichnungen für Rollen

1. Basisdaten ...

- unkritische **allgemeine Daten zum System**
- wird hauptsächlich für die Systemgruppen (z.B. **Display ...**) verwendet

2. Daten ...

- Zugriff auf und damit auch Anzeige von **Daten** (z.B. Theme, Display, direkt per MQTT)
- entweder rein lesend (Endung **... lesen**) oder inkl. Bedienung (Endung **... lesen und bedienen**)
- bei MQTT Objekten (Ladepunkte, Fahrzeug SoC, Komponenten wtc.) zusätzlich eine Rolle **... MQTT-Input**, um das jeweilige Objekt von extern mit Daten zu beschreiben

3. Einstellungen ...

- Zugriff auf die jeweilige **Seite der Einstellungen** mit allen dort benötigten Rechten
- Beispiel: **Einstellungen: Konfiguration - Fahrzeuge** erlaubt den Zugriff auf sämtliche Fahrzeuge und Profile
- Ausnahmen: **Status, Auswertungen - Ladeprotokoll, Auswertungen - Diagramme** zeigen nur die Daten an, für welche durch zusätzliche Rollen Leserechte erteilt wurden.

Beispiel der Rolleneigenschaften

- Feld **Rollenname**: die technische Bezeichnung der Rolle im Backend
- Feld **Beschreibung**: Kurzbeschreibung dieser Rolle, nicht immer vorhanden, Einschränkung der Schnittstelle
- blauer Infokasten: Detailliertere Beschreibung der Rolle, nicht immer vorhanden, Einschränkung der Schnittstelle
- Feld **Zugriffsrechte (ACLs)**:
 - Auflistung der einzelnen Rechte dieser Rolle
 - „Empfangen erlaubt“ heißt, dass die Daten bereitgestellt und eingesehen werden können (Leserechte)
 - „Veröffentlichen erlaubt“ heißt, dass Daten geschrieben werden dürfen (Schreibrechte)

Basisdaten: Display
>

Basisdaten: Hauptseite/Theme
v

Rollenname →

Beschreibung →

Zugriffsrechte (ACLs) ⓘ →

basic-theme-data

Basisdaten zum Laden eines Themes

Diese Rolle ermöglicht das Auslesen grundlegender Einstellungen des Systems und wird verwendet, um das konfigurierte Theme zu laden. Notwendig für die anonyme Gruppe!

"openWB/counter/get/hierarchy" -> Empfangen erlaubt
"openWB/general/web_theme" -> Empfangen erlaubt

Basisdaten: System
>

Typische Anwendungsfälle

Einstellungen mit Kennwort sichern

- Nach Aktivierung der Benutzerverwaltung ist nur noch **passwortgeschützter Zugang** zum openWB-EMS erlaubt. Dies gilt für den Administrator genauso wie für die normalen Nutzer.
- Für den **vollen Zugriff** auf die Einstellungen kann **admin** oder ein eigener Benutzer mit der Rolle **Voller Zugang lesen und schreiben** verwendet werden.
- Die Gruppe **anonymous** kann mit **weiteren oder allen Rollen** für Daten erweitert werden, sodass **alle Daten** eingesehen und **Ladepunkte** bedient werden können.

Benutzerverwaltung WEG mit Ladepunkten

Kurzanleitung

1. für jede Wohnung/Ladepunkt eine Gruppe mit passenden Rollen anlegen (=Lese-/Bedienrechte)
2. Rechte für Fahrzeuge entweder ebenfalls in diese Gruppe oder auf der Benutzerebene zuordnen
3. dem jeweiligen „Display-...“ Benutzer diese Gruppe(-n) zuordnen
4. Benutzer für jede Wohnung erstellen und ebenfalls diese Gruppe(-n) zuordnen
5. ggf. weitere Rollen für Status, Ladeprotokoll und Diagramme ergänzen

Detaillierte Anleitung f. 3 Bewohner (1 Nutzer je einer Wohnung)

Empfehlung

- je Wohnung eine Gruppe anlegen
- Benutzer anlegen und der passenden Gruppe zuordnen

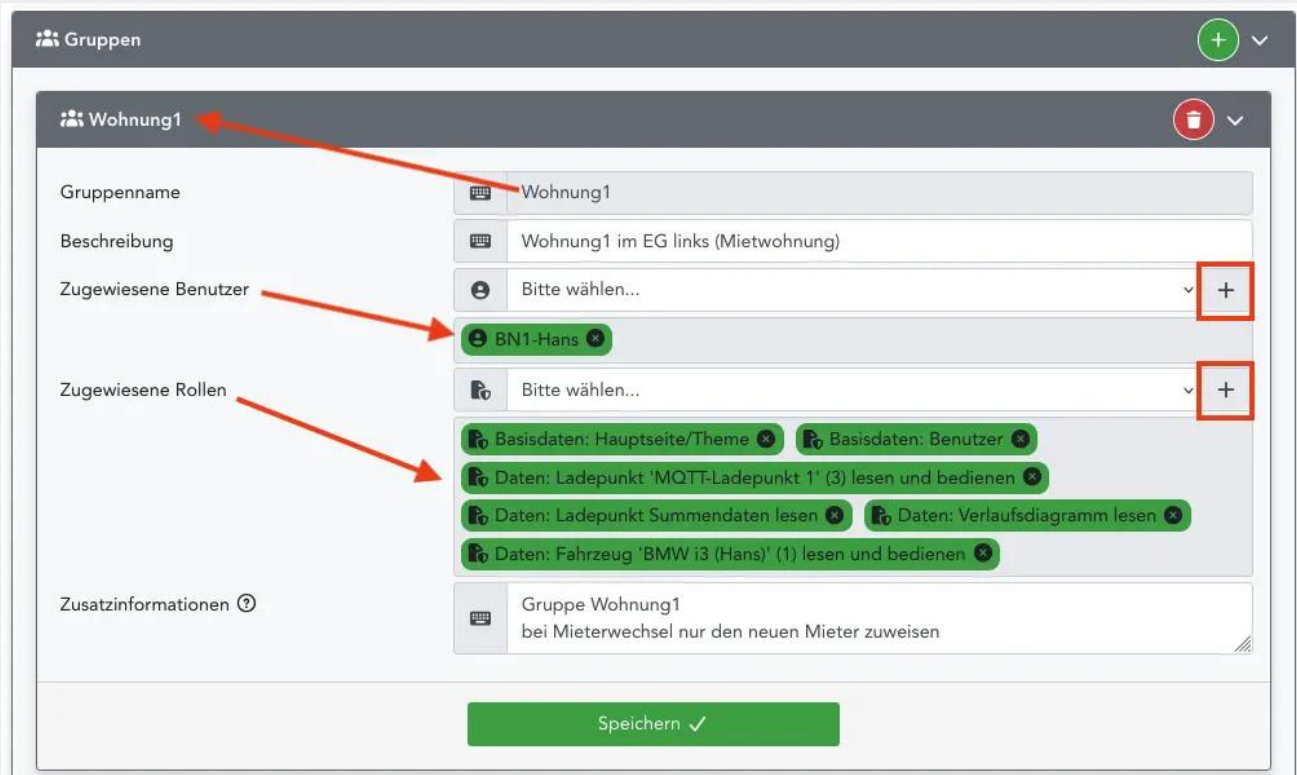
Vorteile

- Mehrere Benutzer einer Wohnung (z.B. Familie) können identisch eingerichtet werden.
- Bei einem Mieter-/Eigentümerwechsel muss nur der neue Benutzer der zugehörigen (Wohnungs-)Gruppe zugeordnet werden.

Zuerst werden unter **Gruppen** 3 individuelle Gruppen mittels +Zeichen (rechts) für die 3 Wohnungen angelegt:



Im Anschluss werden den Gruppen die jeweils gültigen **Rollen** zugewiesen. Hier am Beispiel der **Wohnung1**. Speichern nicht vergessen!



Rollen für eine **Wohnungs-Gruppe**

- **Basisdaten: Benutzer**
- **Basisdaten: Hauptseite/Theme** , um alle notwendigen Daten für die Bedienung über die Webseite zu erteilen
- **Daten: Ladepunkt XYZ lesen und bedienen** für alle zugewiesenen LP, ermöglicht Ansicht der Daten und Bedienung (z.B. sperren etc.)
- **Daten: Fahrzeug XYZ lesen und bedienen** für alle Fahrzeuge dieser Wohnung, ermöglicht die Zuordnung zum LP und z.B. Eingabe des man. SoC
- **Daten: Verlaufsdiagramm lesen** , um die Daten im Diagramm anzuzeigen
- **Daten: Ladepunkt Summendaten lesen** , um die Ladedaten in den Tagessummen anzuzeigen

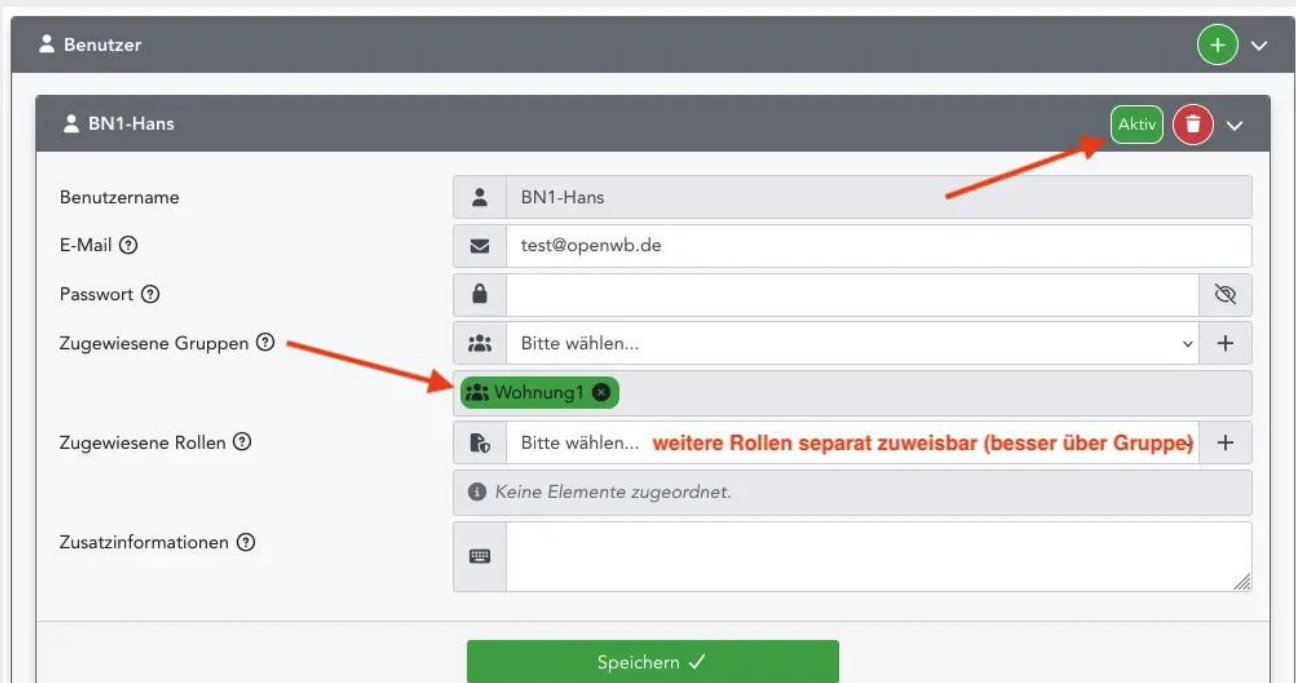
Optional weitere Rollen zuordnen:

- Zugriff auf Daten:
 - Falls es einen eigenen Wohnungszähler gibt: **Daten: Zähler XYZ lesen**
 - Falls EVU-Daten angezeigt werden sollen: **Daten: Zähler 'EVU Zähler' lesen**
 - Falls PV-Daten angezeigt werden sollen: **Daten: Wechselrichter Summendaten lesen** oder **Daten: Wechselrichter XYZ lesen**
 - analog für **Speicher** oder die **Ladepunkt-Summendaten**
- Zugriff auf Einstellungen:
 - Jede einzelne Seite kann individuell freigegeben werden.
 - Status freigeben: **Einstellungen: Status** , Dort werden nur die Komponenten angezeigt, für welche Rechte (**Daten: ... lesen**) erteilt wurden.
 - Ladeprotokoll: **Einstellungen: Auswertungen - Ladeprotokoll**
 - Diagramme: **Einstellungen: Auswertungen - Diagramme**

Nun werden die 3 Bewohner unter **Nutzer** mittels +Zeichen (rechts) angelegt.



Im Anschluss wird den Nutzern die jeweilige **Gruppe** (Wohnung) zugewiesen. Hier am Beispiel des Nutzers **BN1-Hans**. Speichern nicht vergessen!



Für jede openwb, die potentiell ein Display haben kann, werden automatisch Benutzer mit dem Namen **Display-<IP>** bzw. **Display-Intern** für das Display der primary angelegt. Diese Benutzer haben **noch keine Zugriffsrechte!**

Im Normalfall bekommt das Display auch Zugriff auf **seine** Ladepunkte und Fahrzeuge über die entsprechenden Rollen **Daten: Ladepunkt/Fahrzeug XYZ lesen und bedienen**. Ist alles

konfiguriert, müssen die Displays der secondaries **einmalig neu gestartet** werden. Entweder über einen **soften Reboot** oder **durch kurzes Aus- und wieder Einschalten des Displays in den Einstellungen der secondary**.

Display-Intern Aktiv

Benutzername: Display-Intern

Zugewiesene Gruppen: display

Zugewiesene Rollen: Daten: Ladepunkt 'LP 3' (5) lesen und bedienen, Daten: Ladepunkt '6' (6) lesen und bedienen

Zusatzinformationen

Speichern ✓

Bedienung an diesem Display wird für diese Ladepunkte freigegeben

From:
<https://wiki.openwb.de/> - openWB GmbH & Co. KG

Permanent link:
<https://wiki.openwb.de/doku.php?id=openwb:vc:2.3.x:software:einstell-konfig:system:sicherheit:benutzerverwaltung>

Last update: 2026/10/28 21:54

