FORCAM FORCE IIOT
Benutzerverwaltung

Version 5.11

Handbuch

Dokument: Handbuch - FORCAM FORCE IIOT Benutzerverwaltung.docx

Freigabedatum: 05.05.22

Dokumentversion: 1

Autor: Ali Egilmez

FB_8-41 ERSTELLT AM: 22.03.22 GEÄNDERT AM: 05.05.22 VERSION: V1
FREIGEGEBEN DURCH: HEAD OF TTE AUTOR: TECHNICAL WRITER VERTRAULICHKEITSSTUFE: ÖFFENTLICH

Inhaltsverzeichnis

1 Konzept*

Die Workbench ist eine mehrsprachige, webbasierte Anwendung für die Konfiguration der Stammdaten und anderen Terminal-spezifischen Einstellungen. Die Workbench wird dazu verwendet, FORCAM FORCE IIOT zu konfigurieren.

Dieses Handbuch bietet einen Überblick und eine Anleitung für folgende grundlegende Konfigurationsmöglichkeiten der Workbench:

- Benutzer anlegen
- Rechte und Rollen vergeben
- Passwort-Richtlinien definieren

Weitere Funktionen werden in gesonderten Handbüchern behandelt, die von FORCAM ebenfalls bereitgestellt werden.

* Aus Gründen der besseren Lesbarkeit wird im Text verallgemeinernd das generische Maskulinum verwendet. Diese Formulierungen umfassen jedoch gleichermaßen alle Geschlechter und sprechen alle gleichberechtigt an.

2 Benutzer-Editor

Pfad: Benutzerverwaltung > Benutzer-Editor

Jedem Benutzer der Workbench kann ein eigenes Benutzerkonto angelegt werden. Einem Benutzerkonto können eine oder mehrere Rollen zugewiesen werden. Die Zuweisung einer Rolle ist dabei nicht obligatorisch.

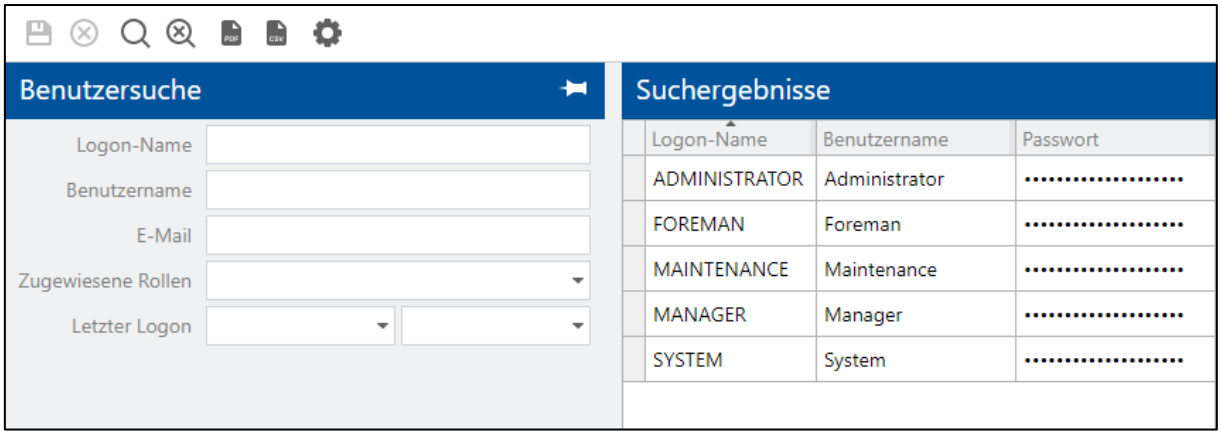

Bild 1: Benutzer-Editor

Um ein neues Benutzerkonto zu erstellen:

1. Im rechten Bereich unter Suchergebnissen rechtsklicken und im Kontextmenü auf **Neuen Benutzer erstellen** klicken.
2. Gewünschte Daten eintragen (s.u.).
   Die mit einem blauen Punkt markierten Felder sind Pflichtfelder.
3. Speichern.

ⓘ Ein Superuser hat Zugriff auf alle Funktionen des Systems.

ⓣ Änderungen am Benutzerkonto können Sie direkt in der Tabelle der Suchergebnisse vornehmen.

Folgende Felder bzw. Einstellungen sind möglich:

Tabelle 1: Parameter für die Konfiguration eines Benutzerkontos in FORCAM FORCE IIOT

Feld	Beschreibung
Login-Name	Pflichtfeld. Name, mit dem sich der Benutzer in der Workbench anmeldet. Erscheint nach der Anmeldung im rechten oberen Bildschirmrand. Für den Namen sind folgende Zeichen erlaubt: Großbuchstaben, Ziffern und Unterstrich (_).
Benutzername	Pflichtfeld. Name, der als zusätzliche Information zum Konto gespeichert wird. Kann aus beliebigen Zeichen bestehen.
Passwort	Pflichtfeld. Passwort, das neben dem Login-Namen bei der Anmeldung in die Workbench eingegeben werden soll. Kann aus beliebigen Zeichen bestehen und beliebig lang sein, solange keine Passwort-Regel angewendet wird (s.u.).
E-Mail	Mailadresse, das dem Konto hinterlegt werden soll. Wird bspw. verwendet, um dem Benutzer eine Benachrichtigung etwa bei Grenzwertverletzungen zu schicken.

Feld	Beschreibung
Benutzer gesperrt	Gibt an, ob das Konto gesperrt ist. Ein Konto wird gesperrt, wenn das Passwort zu oft falsch eingegeben wird. Die Anzahl der Fehlversuche ist in den Passwort-Regeln konfiguriert. Ein Superuser kann ein Konto entsperren, indem er auf das gesperrte Konto rechtsklickt und im Kontextmenü auf **Benutzer entsperren** klickt.
Passwort-Regeln anwenden	Ist ein Haken gesetzt, gelten alle konfigurierten Passwort-Regeln für dieses Konto.
Passwort änderbar	Ist ein Haken gesetzt, darf das Passwort vom entsprechenden Benutzer selbst geändert werden. Ein Superuser darf jedes Passwort ändern.
Superuser	Ist ein Haken gesetzt, wird das Konto zu einem Superuser. Ein Superuser hat weitreichende Rechte und kann sämtliche Bereiche der Workbench betreten und alle möglichen Aktionen durchführen.
Zugewiesene Rollen	Rollen, die dem Konto zugewiesen sind (s.u.). Rechte und Rollen werden im Rechte- & Rollen-Editor konfiguriert (siehe Kapitel 3).
Zeitzone	Zeitzone des Kontos
Letzter Login	Datum, an dem der Benutzer sich zuletzt angemeldet hat
Lokalisierung	Lokalisierung für das Konto (siehe Abschnitt 2.1). Eine Lokalisierung des Kontos ist obligatorisch, wenn diese definiert wurde.

Um einem Benutzerkonto eine Rolle zuzuweisen:

✓ Ein Benutzerkonto ist bereits angelegt und gespeichert.

1. Auf gewünschtes Benutzerkonto rechtsklicken und im Kontextmenü auf **Rollenzuweisungen bearbeiten** klicken.

➔ Die Ansicht wechselt in den Rollen-Editor.

2. Im linken oberen Bereich **Rollen** rechtsklicken und im Kontextmenü auf **Rollen zuweisen** klicken.
3. Im Folge-Dialog die gewünschten Rollen auswählen und bestätigen.
   Sie können einem Benutzerkonto auch mehrere Rollen zuweisen.
4. Im rechten oberen Bereich **Organisatorische Einheiten** rechtsklicken und im Kontextmenü auf **Organisatorische Arbeitsplatzeinheit hinzufügen** klicken.
5. Im Folge-Dialog die gewünschte Arbeitsplatz-Hierarchie auswählen und bestätigen.
6. Im Bereich **Organisatorische Einheiten** rechtsklicken und im Kontextmenü auf **Organisatorische Personaleinheit hinzufügen** klicken.
7. Im Folge-Dialog die gewünschte Person bzw. Kostenstelle auswählen und bestätigen.
8. Speichern.

ⓘ Der untere Bereich **Zugewiesene Rechte** gibt alle Rechte für die ausgewählte Rolle in einer detaillierten Baumstruktur an.

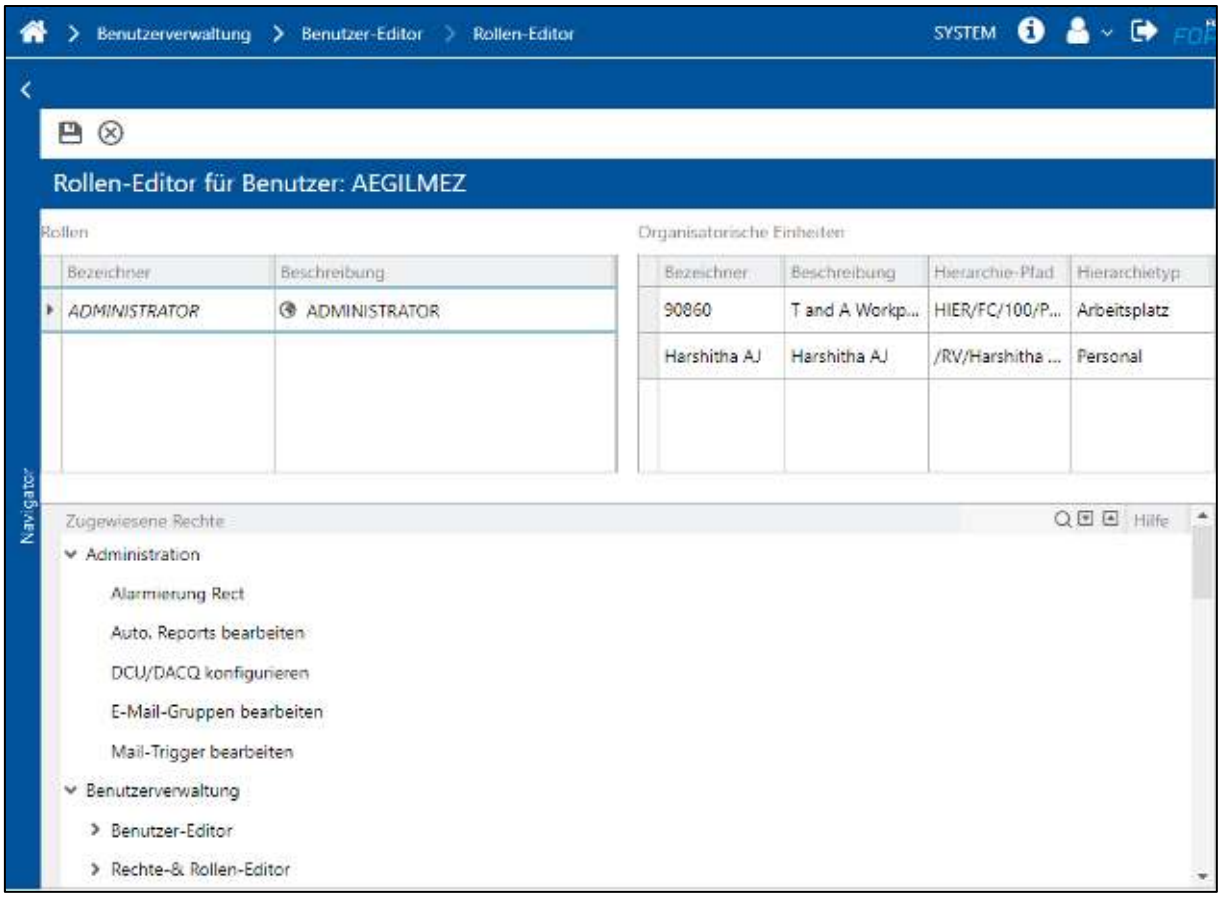

Bild 2: Rollen-Editor

2.1 Lokalisierung

Wird die Multi-Site Administration aktiv verwendet, müssen grundsätzlich alle Benutzer lokalisiert werden. Es können nur lokalisierte Benutzer und Superuser existieren.

ⓘ Für detaillierte Informationen zu Multi-Site siehe das Handbuch Multi-Site Administration.

Einem Benutzer werden bei der Lokalisierung Instanzen der definierten Lokalisierungsebene für Multi-Site zugeteilt. Die Instanzen der Lokalisierungsebene aus der ORG-Hierarchie besitzen zugewiesene konfigurierte Attribute.
Ein Superuser kann lokale Administratoren erzeugen, indem er Benutzer lokalisiert. Ein Superuser hat keine Einschränkungen auf die Einsicht von Daten und hat Zugriff auf sämtliche Lokalisierungen.
Ein lokalisierter Benutzer kann nur seine ihm selbst zugewiesenen Lokalisierungen sehen. Er erhält grundsätzlich Anzeige-, Editier- und Erzeugungsrechte basierend auf dem bestehenden Rechte- & Rollenmanagement.
Beispiel:
In einer ORG-Hierarchie gibt es die Lokalisierung **GER** (Deutschland). Die Arbeitsplätze **760-1** und **760-2** wurden dem Unterknoten **MUC** (München) zugewiesen. In der Benutzerverwaltung wurden den Benutzern die Lokalisierung **GER** zugewiesen. Diese beiden Nutzer können nur Daten sehen und editieren, die auf den Standort München lokalisiert sind.

ⓘ Ein lokaler Administrator muss mindestens eine, kann jedoch auch mehrere Lokalisierungen haben.

Suchergebnisse

Logon-Name	Benutzername	Passwort	E-Mail	Lokalisierung	Super-User
ADMINISTRATOR	Administrator	••••••	Administrator@example.com	LON	☐
FOREMAN	Foreman	••••••	FOREMAN@example.com	LON	☐
JGANDHI	Jiten Gandhi	•			☑
JGTEST01	JGTets01	•		RAV	☐
MAINTENANCE	Maintenance	••••••	MAINTENANCE@example.com	RAV	☐
MANAGER	Manager	••••••	MANAGER@example.com	RAV	☐
SYSTEM	System	••••••	System@example.com	RAV	☐

Bild 3: Lokalisierung von Benutzern

Ein lokaler Administrator kann mit entsprechenden Rechten andere Benutzer lokalisieren, sofern diese Teil seiner eigenen Lokalisierung sind. Ein Benutzer kann auch eine fremde Lokalisierung (Fremdschlüssel) tragen.
Bei der Bearbeitung von Lokalisierungen anderer Benutzer kann ein lokaler Administrator ausschließlich seine eigene Lokalisierung weitergeben oder entfernen. Legt er selbst weitere Benutzer an, teilen sie ebenfalls automatisch seine Lokalisierungen.
Beispiel:
Ein Superuser lokalisiert Benutzer X auf Werk A. X ist lokaler Administrator für Werk A.
X lokalisiert Benutzer Y. Y ist damit ebenfalls lokaler Administrator für Werk A.
Y erstellt Benutzer Z. Z ist kein Administrator, jedoch automatisch Werk A zugehörig.

ⓘ Ein Benutzer darf nur die Stammdaten seiner eigenen Lokalisierung verwalten.

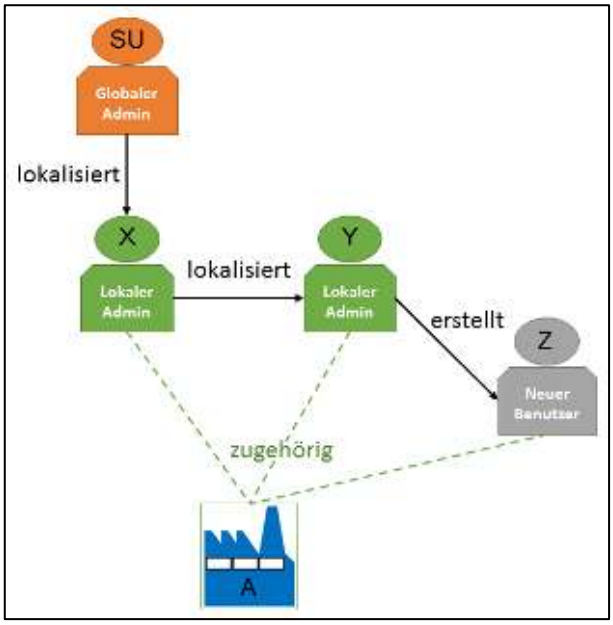

Bild 4: Lokalisierung von Benutzern (Beispiel)

Um einen Benutzer zu lokalisieren:

- ✓ Die ORG-Hierarchie ist konfiguriert.
- ✓ Ein Hierarchie-Baum ist angelegt.

1. Beim gewünschten Benutzer in der Spalte **Lokalisierung** das Drop-down-Menü öffnen.
2. Im Folgedialog die gewünschten Lokalisierungen auswählen und bestätigen.
3. Speichern.

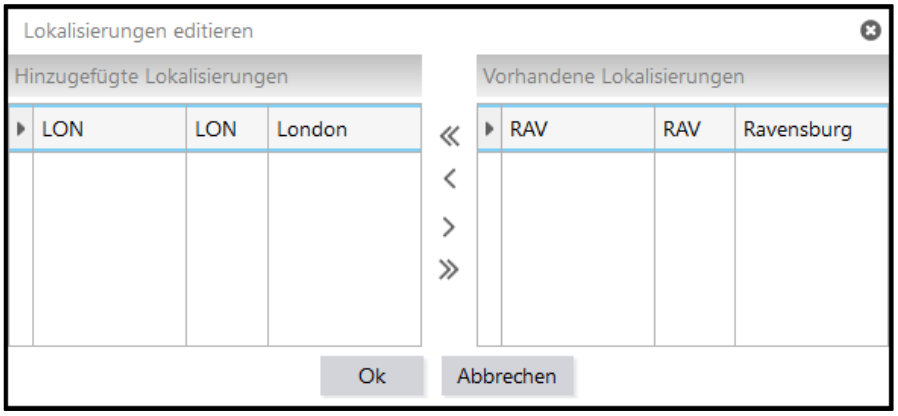

Bild 5: Benutzer-Lokalisierung hinzufügen

ⓘ Ein Superuser hat keine Lokalisierung. Er ist dadurch globaler Administrator und in Rechten nicht eingeschränkt.

3 Rechte- & Rollen-Editor

Pfad: Benutzerverwaltung > Rechte- & Rollen-Editor

Benutzer von FORCAM FORCE IIOT können in verschiedene Gruppen mit unterschiedlichen Rechten eingeteilt werden. Diese Gruppen werden als Rollen bezeichnet (z. B. Manager, Vorarbeiter, Wartung etc.). Jeder Rolle können die Rechte bzw. Funktionen zugewiesen werden, die sie für ihre jeweilige Aufgabe benötigt. Nicht zugewiesene Rechte können entsprechend von der jeweiligen Rolle nicht ausgeübt werden.

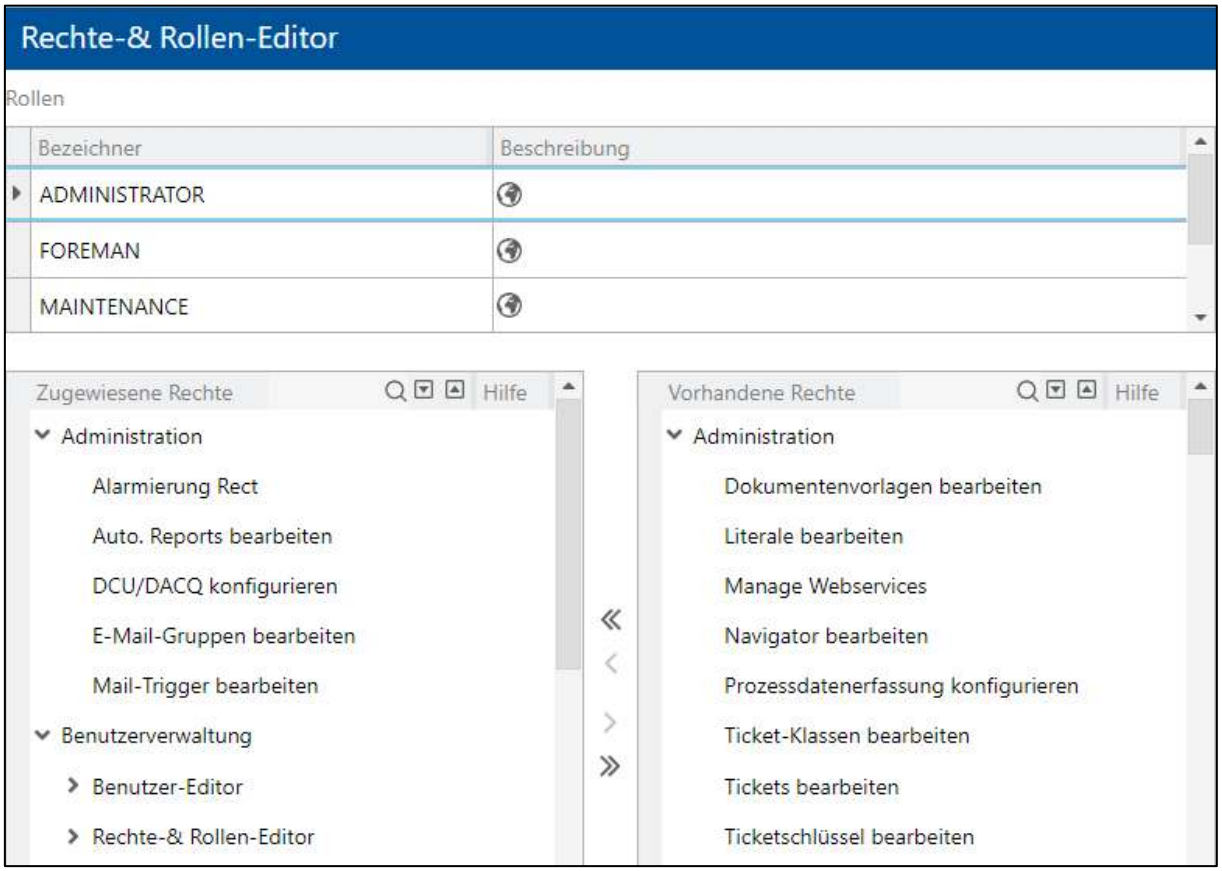

Bild 6: Rechte- & und Rollen-Editor

Die Verwendung des Rechte- und Rollenmanagements ist notwendig, um die Sichtbarkeit und Pflege von Daten und Benutzeroberflächen grundsätzlich innerhalb von FORCAM FORCE IIOT zu handhaben.

Ein lokaler Administrator benötigt zwingend die Zuweisung der organisatorischen Einheit, auf die er lokalisiert ist (erforderliche Zweige der ORG-Hierarchie der Lokalisierung). Die Zuweisung entscheidend grundlegend darüber, welche Hierarchie und Zweige einer Hierarchie der Benutzer sehen und an Benutzer in Rollen weitergeben (zuweisen) darf.

ⓘ Für detaillierte Informationen zu Multi-Site siehe das Handbuch Multi-Site Administration.

Um eine neue Rolle zu erstellen:

1. Im oberen Bereich unter **Rollen** rechtsklicken und im Kontextmenü auf **Neue Rolle anlegen** klicken.
2. Optional: Beschreibung eintragen.
3. Speichern.

Um einer Rolle Rechte zuzuweisen:

✓ Eine Rolle ist definiert.

1. Im oberen Bereich unter **Rollen** die gewünschte Rolle auswählen.
2. Im unteren rechten Bereich **Vorhandene Rechte** ein oder mehrere Rechte auswählen und über das Verschieben-Icon nach links bewegen.
3. Speichern.

➔ Die Rolle ist mit allen Rechten ausgestattet, die unter **Zugewiesene Rechte** aufgelistet sind.

4 Passwort-Richtlinien

Pfad: Benutzerverwaltung > Passwort-Richtlinien

Die Passwort-Richtlinien bieten die Möglichkeit, individuelle oder kundenspezifische Richtlinien für Benutzerpasswörter festzulegen. Es kann z. B. definiert werden, dass Passwörter bestimmte Zeichen enthalten oder nicht enthalten dürfen oder einer bestimmten Länge entsprechen müssen.

⚠ Die Passwort-Richtlinien betreffen die Dienste Workbench und Office. Das Shopfloor Terminal ist hiervon ausgeschlossen. Passwörter für das Shopfloor Terminal werden in der Profilkonfiguration definiert.

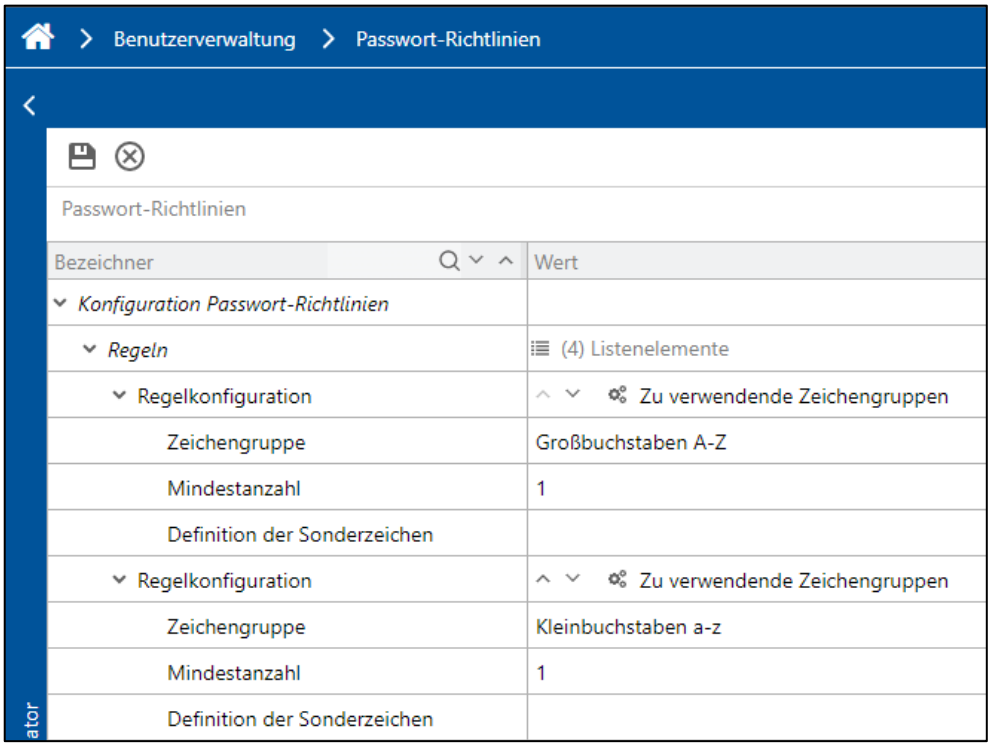

Bild 7: Konfigurierte Passwort-Regeln

Insgesamt stehen elf verschiedene Regeln zur Verfügung. Die Regeln können beliebig kombiniert werden, sind jedoch nicht durch eine Und-Verknüpfung miteinander verbunden. Sind z. B. vier Regeln konfiguriert und der Benutzer verstößt gegen die erste, ist das Passwort bereits ungültig, selbst wenn er die übrigen drei Regeln befolgt.
Das Anwenden der Passwort-Richtlinie für ein Benutzerkonto (siehe Kapitel 2) bezieht sich ebenfalls auf alle konfigurierten Regeln einer Linie.

Um eine Passwort-Regel hinzuzufügen:

1. Im rechten Bereich auf **Listenelemente** rechtsklicken und im Kontextmenü auf **Neues Listenelement anfügen** klicken.

➔ Ein neues Listenelement wird angehängt, ist initial jedoch zugeklappt.

2. Die neue Regel-Zeile über das Aufklapp-Icon am linken Ende öffnen.
3. In der Zeile **Regelkonfiguration** im Drop-down-Menü die gewünschte Passwort-Regel auswählen.

➔ Je nach Auswahl erscheinen andere zusätzliche Parameter.

4. Die ausgewählte Regel anhand der Parameter wie gewünscht definieren.
5. Speichern.

Folgende Regeln werden von FORCAM FORCE IIOT unterstützt:

Tabelle 2: Mögliche Passwort-Richtlinien in FORCAM FORCE IIOT

Regel	Parameter	Beschreibung
Benutzername		Der Benutzername darf nicht im Passwort enthalten sein. Die Groß- und Kleinschreibung spielt dabei keine Rolle.
Erlaubte Zeichen		Zeichen, aus denen das Passwort bestehen oder mit diesen beginnen/enden muss
	Zeichen	Definition von Zeichen für das Match-Verhalten
	Match-Verhalten	Die Regel ändert sich je nach ausgewähltem Match-Verhalten: – Enthält: Das Passwort muss aus den hier definierten Zeichen bestehen und darf keine anderen Zeichen enthalten. – Beginnt mit: Das Passwort muss mit einem der hier definierten Zeichen beginnen. – Endet mit: Das Passwort muss mit einem der hier definierten Zeichen enden.
Fehlgeschlagene Logins		Bestimmt, nach wie vielen fehlgeschlagenen Anmeldeversuchen das Benutzerkonto gesperrt wird.
	Anzahl fehlgeschlagener Logins	Bestimmt die genaue Anzahl an möglichen Fehlversuchen. Ist bspw. 3 eingetragen, wird das Konto nach dem dritten Fehlversuch gesperrt.
Mindest- und maximale Länge		Bestimmt die Zeichenlänge des Passworts
	Mindestlänge	Mindestanzahl an Zeichen des Passworts
	Maximale Länge	Maximale Anzahl an Zeichen des Passworts
Passwort-Gültigkeit		Legt die Gültigkeitsdauer des Passworts fest (z. B. 14 Tage)
	Einheit	Einheit für die Gültigkeitsdauer
	Anzahl Einheiten	Anzahl der Einheiten für die Gültigkeitsdauer

Regel	Parameter	Beschreibung
Passwort-Historie		Das Passwort darf nicht zuvor verwendet worden sein.
	Anzahl Einträge aus Passwort-Historie	Legt fest, wie viele der letzten Passwörter nicht verwendet werden dürfen (z. B. die drei letzten Passwörter)
Regulärer Ausdruck: Akzeptiert Passwort		Das Passwort muss diesem regulären Ausdruck entsprechen, um akzeptiert zu werden.
	Regulärer Ausdruck	Regulärer Ausdruck, dem das Passwort entsprechen muss
Regulärer Ausdruck: Lehnt Passwort ab		Das Passwort darf nicht diesem regulären Ausdruck entsprechen, um akzeptiert zu werden.
	Regulärer Ausdruck	Regulärer Ausdruck, der vom Passwort ausgeschlossen werden soll
Unerlaubte Zeichen		Zeichen, aus denen das Passwort nicht bestehen oder mit diesen beginnen/enden darf
	Zeichen	Definition von Zeichen für das Match-Verhalten
	Match-Verhalten	Die Regel ändert sich je nach ausgewähltem Match-Verhalten: – Enthält: Das Passwort darf keine der hier definierten Zeichen enthalten, sondern muss aus anderen Zeichen bestehen. – Beginnt mit: Das Passwort darf nicht mit einem der hier definierten Zeichen beginnen. – Endet mit: Das Passwort darf nicht mit einem der hier definierten Zeichen enden.
Zahlenbereich		Zahlenbereich, der im Passwort nicht vorkommen darf. Beispiel: Bei einem Bereich zwischen 22 und 33 dürfen keine Zahlensequenzen verwendet werden, die dazwischen liegen (z .B. 23, 32). ⚠ Bei einem Bereich zwischen 0 und 9 dürfen überhaupt keine Zahlen verwendet werden, da jede Zahlensequenz dazwischen liegt.
	Startbereich	Start des Zahlenbereichs
	Endbereich	Ende des Zahlenbereichs
	Match-Verhalten	Bestimmt, an welcher Stelle die Zahl beachtet werden soll

Regel	Parameter	Beschreibung
Zu verwendende Zeichengruppen		Zeichen aus einer Zeichengruppe, die das Passwort enthalten muss. Beispiel: Damit das Passwort einen Großbuchstaben enthalten soll, muss **Großbuchstaben A-Z** mit der Mindestanzahl 1 ausgewählt werden. Pro Regel kann nur eine Zeichengruppe konfiguriert werden. Soll das Passwort zusätzlich eine Zahl beinhalten, muss eine weitere Regel hinzugefügt und dort **Zahlen 0-9** ausgewählt werden.
	Zeichengruppe	Zeichengruppe, aus der das Passwort mindestens n Zeichen enthalten soll
	Mindestanzahl	Mindestanzahl der Zeichen der ausgewählten Gruppe, die das Passwort enthalten muss
	Definition der Sonderzeichen	Bestimmt, welche Zeichen als Sonderzeichen gelten. Nur relevant, wenn als Zeichengruppe **Sonderzeichen** ausgewählt wurde.

5 Anhang

5.1 Dokument-Konventionen

Tabelle 3: Verwendete Schriftarten, Formatierungen und Zeichen

Konvention	Beschreibung
Fettschrift	Die Bezeichnungen von Schaltflächen und Optionen sind fettgeschrieben.
Kursivschrift	Hervorgehobene Wörter sind kursivgeschrieben.
Icons	Bei einer Funktion, die über ein Icon dargestellt ist, wird auf das Icon als Objekt referiert.
Handlungsresultat	Handlungsresultate sind durch ➔ gekennzeichnet.
Voraussetzungen	Voraussetzungen sind durch ✓ gekennzeichnet.
Warnungen	Warnungen sind durch ⚠ gekennzeichnet.
Hinweis	Hinweise sind durch ⓘ gekennzeichnet.
Tipps	Tipps sind durch ⓣ gekennzeichnet.

5.2 Abbildungsverzeichnis