Rollen

Diese Seite beschreibt die Maske po_editRole.act (erreichbar über die Rollen-Übersicht po_showRoles.act). Das Konzept dahinter – Kompetenzziele, Suchstrategie, Organisationstypen – ist im Kapitel Rollen[1] beschrieben.

> NOTIZ
>
> **Berechtigung:** Rollen anlegen, ändern und löschen darf nur, wer Systemadministrator ist oder eine Einsichtsberechtigung auf **alle Mandanten** besitzt. Lokale Administratoren sehen die Maske eingeschränkt: Die Felder Workflow-ID, Standardrolle, Badge und "Vor lokalem Administrator verbergen" sind für sie ausgeblendet, und es öffnet sich direkt der Reiter Rolleninhaber.

Anlegen einer neuen Rolle

- **Neue Rolle**: Maske befüllen und mit "Speichern" bzw. "Speichern & Schließen" bestätigen.
- Die **Reiter** (Workflow Optionen, Aktionen, Rolleninhaber, ...) erscheinen erst **nach dem ersten Speichern**.
- **Gültig von / Gültig bis** der Rolle können nur beim Anlegen gesetzt werden; danach werden sie nur mehr angezeigt.

Felder

- **Name** (Pflicht, mind. 2 Zeichen)
  Name der Rolle. Es wird geprüft, dass es die Rolle für den gewählten Mandanten nicht bereits gibt.
- **Beschreibung**
  Optionale Beschreibung der Rolle.
- **Mandant**
  Mandant, für den die Rolle gilt; ohne Auswahl ist die Rolle mandantenübergreifend.
- **Workflow-ID** (Pflicht)
  Interne Referenz für Genehmigungsprozesse. Das Feld wird automatisch mit dem Rollennamen vorbefüllt und muss **eindeutig** sein ("ParticipantId bereits vergeben"). Erlaubt sind nur Buchstaben, Ziffern und Unterstrich – **keine Satzzeichen, Leerzeichen oder Bindestriche** (Beispiel: VAZ_Verantwortlicher). Im Standardfall soll die Workflow-ID nachträglich **nicht** geändert werden (nur nach Absprache mit Workflow).
- **Standardrolle**
  Ordnet die Rolle einer System-Standardfunktion zu: *Benutzer*, *Vorgesetzter*, *HR Admin*, *Kiosk Admin* oder *System-Administrator*. Pro Mandant darf jede Standardrolle nur einmal vergeben sein.
- **Badge**
  Farbstil, mit dem die Rolle in Oberflächen als Badge dargestellt wird (primary, secondary, success, danger, warning, light, dark).
- **Vor lokalem Administrator verbergen**
  Ist die Option aktiviert, wird die Rolle inklusive aller Zuordnungen bei lokalen Administratoren verborgen.
- **Abgeleitet von Rolle** (nur bei Mandanten-Rollen sichtbar)
  Zeigt die Vorlagen-Rolle, von der diese Mandanten-Rolle abgeleitet wurde (siehe unten).

Reiter Workflow Optionen

- **Antragsteller als Rolleninhaber für sich selbst unterdrücken**
  Relevant, wenn der Antragsteller zugleich Rolleninhaber ist (z.B. Vorgesetzter): Der Antrag geht dann an den stellvertretenden bzw. hierarchisch nächsthöheren Rolleninhaber – verhindert Selbstgenehmigung.

- **Vertreter des Antragstellers als Rolleninhaber unterdrücken**
  Übergeht den Stellvertreter des Antragstellers bei der Suche. **Nur aktivierbar, wenn die vorige Option gesetzt ist.** Vorsicht bei Abteilungen mit nur zwei Mitarbeitern (Vorgesetzter + Stellvertreter # Suche bleibt erfolglos).
- **Hierarchische Gruppe bei Suche nach Rolleninhaber berücksichtigen**
  Ist dieses Flag gesetzt, wird zusätzlich zur direkten Zuordnung auch die hierarchische Gruppe des Antragstellers nach Rolleninhabern durchsucht. Beispiel: Hr. Weiss, Hr. Wagner und Fr. Müller sind Rolleninhaber "Vorgesetzter" für Gruppe G01; Hr. Maier ist Hrn. Müller direkt zugeordnet. Ohne Flag wird nur Hr. Maier gefunden, mit Flag zusätzlich die Rolleninhaber der Gruppe G01.
- **Organisationstyp**
  Bestimmt, in welcher Organisationsstruktur nach Rolleninhabern gesucht wird: *Hierarchische Aufbauorganisation*, *Kostenstellen*, *Projektgruppen*, *Lose Gruppen* oder *Standorte*. Nur beim Typ "Hierarchische Aufbauorganisation" stehen Suchrichtung und Ebenen-Einstellungen zur Verfügung; bei losen Gruppen erfolgt keine hierarchische Befüllung, da keine Verknüpfung der Gruppen untereinander existiert.
- **Max. Anzahl von Rolleninhabern für Workflow**
  Eine Zahl größer 0 beschränkt die aufgelösten Rolleninhaber im Workflow (z.B. 2 # maximal zwei mögliche Vorgesetzte, auch wenn per Vererbung mehr definiert wären).
- **Suchrichtung** (nur bei hierarchischer Aufbauorganisation)
  Keine – Suche nur in der eigenen Gruppe/Abteilung; *Aufwärts* – Suche in übergeordneten Abteilungen (sinnvoll für Vorgesetzten-Rollen); *Abwärts* – Suche in untergeordneten Abteilungen (z.B. Krankmeldung durch Kollegen). Details siehe Rollen[2].
- **Anzahl der Ebenen, um Rolleninhaber zu suchen** (erscheint bei Suchrichtung aufwärts/abwärts)
  Begrenzt die Suche auf die angegebene Zahl von Ebenen.
- **Höchste Ebene, bis zu der gesucht werden darf** (erscheint bei Suchrichtung aufwärts/abwärts)
  Begrenzt die Suche nach oben; über diese Ebene hinaus wird nicht gesucht (oberste Ebene = 1).

NOTIZ

Achtung – Selbstgenehmigung an der Ebenengrenze: Befindet sich der Antragsteller (zugleich Rolleninhaber) in der höchsten erlaubten Suchebene, wird er trotz aktivierter Option "Antragsteller als Rolleninhaber für sich selbst unterdrücken" zum eigenen Vorgesetzten. **Lösung:** dieser Person direkt einen Vorgesetzten zuordnen (Rolle mit Kompetenzziel Person).

Reiter Aktionen

Ordnet den Rolleninhabern Aktionsberechtigungen zu. Über **"Neue Aktionsberechtigung"** wird die Aktion gewählt; die Checkbox **"Vererbte Berechtigungen anzeigen"** blendet zusätzlich Berechtigungen ein, die die Rolleninhaber aus anderen Quellen erhalten.

- **Negativ** Ja/Nein – schließt bei Ja von der Berechtigung aus statt sie zu erteilen.
- **Gültig von – bis** – Zeitraum der Berechtigung (leer = ab heute).
- **Einsichtserlaubnis** – wer darf über diese Aktion eingesehen werden: *eigene Person*, *Orgeinheit*, *Orgeinheit + untergeordnete*, *Rollenkompetenz* (Einsicht gemäß den Kompetenzzielen der Rolle), *eigener Mandant*, *alle Mandanten*.
- **Berechtigung/Einsicht an untergeordnete Gruppen vererben** – bei Ja erhalten bzw. betreffen auch die untergeordneten Gruppen die Berechtigung/Einsicht.

Die Liste zeigt je Berechtigung außerdem Modul, Anzahl der betroffenen User, Kompetenzziel und die Herkunft ("Zugeordnet von") und lässt sich filtern und sortieren.

Reiter Rolleninhaber

Zeigt die bestehenden Zuordnungen (mit erweiterter Suche nach Kompetenzziel, Rolleninhaber und Typ) und erlaubt neue über **"Neuer Rolleninhaber"**:

- **Kompetenzziel** – wer darf eingesehen werden: *Alle* (nur mit Einsicht auf alle Mandanten wählbar), eine bestimmte *Person*, *Gruppe* oder ein *Mandant*. Zur Auswahl stehen nur Ziele, für die der Bearbeiter selbst Einsichtsberechtigung hat.
- **Rolleninhaber** – *Person*, *Gruppe* (alle Personen der Gruppe werden Rolleninhaber) oder *Dynamische Rollenzuordnung*. Bei dynamischer Zuordnung wird der Inhaber zur Laufzeit aus dem Kontext des Kompetenzziels bestimmt:
  - *Eigene Orgeinheit* – alle Personen derselben hierarchischen Gruppe (klassischer Fall "Rolle Kollege")
  - *Eigene Orgeinheit + untergeordnete OE's*
  - *Eigener Mandant*
  - *Alle Mandanten* (nur mit entsprechender Einsichtsberechtigung)
- **Gültig von – bis** – Gültigkeitszeitraum der Zuordnung.
- **Reihung** – 1 = primärer Rolleninhaber (z.B. Vorgesetzter), 2 = Stellvertreter, 3, 4, ... weitere Stellvertreter (siehe Stellvertreterregelung[3]). Änderung über das Bearbeiten-Icon der Zeile.

Beim **Bearbeiten** einer bestehenden Zuordnung sind Reihung (bzw. der dynamische Typ) und Gültig-bis änderbar; Gültig-von nur, solange es in der Zukunft liegt. Beim **Löschen** einer aktuell gültigen Zuordnung wird diese mit sofortiger Wirkung beendet (Gültig-bis = jetzt); erst in der Zukunft beginnende Zuordnungen werden tatsächlich entfernt.

Reiter Abgeleitete Mandanten-Rollen

Eine Rolle kann als **Vorlage** für mandantenspezifische Rollen dienen. Über **"Neue Mandantenrolle"** wird pro Mandant eine abgeleitete Rolle erzeugt (Namensvorschlag: Vorlagenname + Mandant; pro Mandant nur eine Ableitung). Abgeleitete Rollen zeigen eine reduzierte Maske – im Wesentlichen den Aktionen-Reiter – und übernehmen die übrigen Eigenschaften von der Vorlage; das Feld "Abgeleitet von Rolle" verweist zurück. Die Liste zeigt alle Ableitungen mit Mandant und Sprung-Link.

Reiter Zugriffsrechte

Vergibt technische Zugriffsrechte (z.B. auf REST-Endpunkte) an die Rolleninhaber:

- **Rollenspezifische Zugriffsrecht-Sets** – Zuordnung vordefinierter Sets (mit Sprung-Link zur Set-Pflege).
- **Rollenspezifische Zugriffsrechte** – einzelne Rechte mit Selektor, Privileg und optionalem Verbieten.

Reiter Workflow Aufgaben

Bei lizenziertem Workflow-Modul erscheint zusätzlich der Reiter **Workflow Aufgaben**: Er zeigt die offenen Aufgaben-Zuordnungen der Rolle und ermöglicht deren Neubewertung (z.B. nach Änderungen an Rolleninhabern).

Suchen, Bearbeiten, Löschen

- **Suche** in der Übersicht nach Name, Beschreibung und Mandant; die Spalten Standardrolle und Workflow-ID sind ebenfalls filterbar. Das Editier-Icon öffnet die Detailansicht.
- **Bearbeiten**: Alle oben beschriebenen Felder und Reiter; die Workflow-ID im Standardfall nicht ändern.

- **Löschen** (nur Systemadministrator): Nach Sicherheitsabfrage wird die Rolle entfernt; bestehende Rolleninhaber-Zuordnungen und Kompetenzen werden dabei mit gestrigem Datum beendet (historisiert), nicht physisch gelöscht.

Felder

Name	Wert
Modul	Portal & Organisation (po)
Webdesk Actionname	po_editRole
Artefakt-Typ	Action

1. /daisy/personalwolke-admin/2640-dsy.html
2. /daisy/personalwolke-admin/2640-dsy.html
3. /daisy/personalwolke-admin/2163-dsy.html