Working with Roles

This page describes the form po_editRole.act (reached via the roles overview po_showRoles.act). The underlying concept – competence targets, search strategy, organization types – is described in the chapter Roles[1].

NOTIZ

Permission: Only system administrators or users with a view permission on **all clients** may create, change or delete roles. Local administrators see a restricted form: the fields workflow ID, default role, badge and "hide from local administrator" are hidden for them, and the role holders tab opens directly.

Creating a new role

- **New role**: fill in the form and confirm with "Save" or "Save & Close".
- The **tabs** (workflow options, actions, role holders, ...) only appear **after the first save**.
- **Valid from / valid to** of the role can only be set at creation; afterwards they are display-only.

Fields

- **Name** (required, min. 2 characters)
  Name of the role. The system checks that the role does not already exist for the selected client.
- **Description**
  Optional description of the role.
- **Client**
  Client the role applies to; without a selection the role is cross-client.
- **Workflow ID** (required)
  Internal reference for approval processes. The field is pre-filled automatically with the role name and must be **unique** ("ParticipantId already in use"). Only letters, digits and underscore are allowed – **no punctuation, spaces or hyphens** (example: VAZ_Verantwortlicher). Normally the workflow ID should **not** be changed afterwards (only after consultation with Workflow).
- **Default role**
  Assigns the role to a system standard function: *user*, *manager*, *HR admin*, *kiosk admin* or *system administrator*. Each default role may only be assigned once per client.
- **Badge**
  Color style used to render the role as a badge in user interfaces (primary, secondary, success, danger, warning, light, dark).
- **Hide from local administrator**
  When enabled, the role including all its assignments is hidden from local administrators.
- **Derived from role** (visible only for client roles)
  Shows the template role this client role was derived from (see below).

Workflow options tab

- **Suppress requester as role holder for themselves**
  Relevant when the requester is also a role holder (e.g. a manager): the request then goes to the deputy or hierarchically next role holder – prevents self-approval.
- **Suppress requester's deputy as role holder**
  Skips the requester's deputy during the search. **Can only be enabled when the previous option is checked.** Beware of departments with only two members (manager + deputy # the search finds nobody).

- **Include hierarchical group when searching for role holders**
  When set, the requester's hierarchical group is searched in addition to direct assignments. Example: Mr. Weiss, Mr. Wagner and Ms. Müller hold the role "manager" for group G01; Mr. Maier is directly assigned to Mr. Müller. Without the flag only Mr. Maier is found, with the flag also the role holders of group G01.
- **Organization type**
  Determines the organization structure searched for role holders: *hierarchical organization*, *cost centers*, *project groups*, *loose groups* or *locations*. Search direction and level settings are only available for the type "hierarchical organization"; loose groups have no hierarchy, so no hierarchical resolution takes place.
- **Max. number of role holders for workflow**
  A number greater than 0 limits the resolved role holders in a workflow (e.g. 2 # at most two possible managers, even if inheritance would yield more).
- **Search direction** (hierarchical organization only)
  None – search only within the own group/department; *upwards* – search in superordinate departments (useful for manager roles); *downwards* – search in subordinate departments (e.g. sick note by colleagues). Details in Roles[2].
- **Number of levels to search for role holders** (appears for upwards/downwards)
  Limits the search to the given number of levels.
- **Highest level up to which may be searched** (appears for upwards/downwards)
  Limits the search towards the top; no search beyond this level (top level = 1).

NOTIZ

Caution – self-approval at the level boundary: If the requester (who is also a role holder) sits in the highest allowed search level, they become their own manager despite the enabled option "suppress requester as role holder for themselves". **Solution:** assign that person a manager directly (role with competence target person).

Actions tab

Assigns action permissions to the role holders. Choose the action via **"New action permission"**; the checkbox **"Show inherited permissions"** additionally displays permissions the role holders receive from other sources.

- **Negative** yes/no – if yes, excludes from the permission instead of granting it.
- **Valid from – to** – validity period of the permission (empty = from today).
- **View permission** – who may be viewed through this action: *own person*, *org unit*, *org unit + subordinated*, *role competence* (view according to the role's competence targets), *own client*, *all clients*.
- **Inherit permission/view to subordinated groups** – if yes, subordinated groups also receive or are covered by the permission/view.

The list additionally shows module, number of affected users, competence target and origin ("assigned from") per permission, and can be filtered and sorted.

Role holders tab

Shows the existing assignments (with extended search by competence target, role holder and type) and allows new ones via **"New role holder"**:

- **Competence target** – who may be viewed: *all* (selectable only with all-clients view permission), a specific *person*, *group* or a *client*. Only targets the editor has view permission for are offered.

- **Role holder** – *person*, *group* (all persons of the group become role holders) or *dynamic role assignment*. With a dynamic assignment the holder is determined at runtime from the competence target's context:
  - *Own org unit* – all persons of the same hierarchical group (the classic "colleague" role)
  - *Own org unit + subordinated org units*
  - *Own client*
  - *All clients* (only with the corresponding view permission)
- **Valid from – to** – validity period of the assignment.
- **Ranking** – 1 = primary role holder (e.g. manager), 2 = deputy, 3, 4, ... further deputies (see deputy rules[3]). Change via the row's edit icon.

When **editing** an existing assignment, ranking (or the dynamic type) and valid-to are changeable; valid-from only while it lies in the future. When **deleting** a currently valid assignment, it is ended immediately (valid-to = now); assignments starting in the future are actually removed.

Derived client roles tab

A role can serve as a **template** for client-specific roles. Via **"New client role"** a derived role is created per client (name proposal: template name + client; only one derivation per client). Derived roles show a reduced form – essentially the actions tab – and inherit the remaining properties from the template; the field "derived from role" points back. The list shows all derivations with client and jump link.

Access rights tab

Grants technical access rights (e.g. to REST endpoints) to the role holders:

- **Role-specific access right sets** – assignment of predefined sets (with jump link to set maintenance).
- **Role-specific access rights** – individual rights with selector, privilege and optional deny.

Workflow assignments tab

With a licensed workflow module, the additional tab **workflow assignments** appears: it shows the role's open task assignments and allows re-evaluating them (e.g. after changes to role holders).

Searching, editing, deleting

- **Search** in the overview by name, description and client; the columns default role and workflow ID are filterable as well. The edit icon opens the detail view.
- **Editing**: all fields and tabs described above; normally do not change the workflow ID.
- **Deleting** (system administrator only): after a confirmation prompt the role is removed; existing role holder assignments and competences are ended with yesterday's date (historicized), not physically deleted.

Felder

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

1. /daisy/personalwolke-admin/2640-dsy.html?language=4

2. /daisy/personalwolke-admin/2640-dsy.html?language=4
3. /daisy/personalwolke-admin/2163-dsy.html?language=4