6. How to Edit a Role

Over time, your organization’s needs may evolve: you might need to grant additional permissions to an existing role or tighten access in response to security changes. The **Edit Role** function lets you fine-tune an existing role’s permissions—adding or removing rights, switching templates, or even upgrading someone’s capabilities—without having to recreate the role from scratch.

Step-by-Step Process

1. Open the Roles Module
From the main navigation menu, select **Roles**.
You’ll see the full list of roles along with their current modules and access scopes.

2. Locate the Role to Edit
Scroll or search to find the role you wish to modify.
Each row shows the summary of the modules it can access.

3. Launch the Edit Dialog
In that role’s Actions column, click the **Edit** (pencil) icon.
The **Edit Role** panel appears, displaying the role’s configuration fields.

4. Review the Role Name and Template
Template dropdown lets you reassign a different predefined template (e.g., Agent, Desk manager, Project admin). Changing the template will replace the permission matrix with the template’s defaults.

5. Adjust “All rights” Toggle (Optional)
Enabling **All rights** immediately grants every possible permission across all modules. This is rarely recommended—use only for super-admin or audit roles.

6. Modify View Permissions
In the **View** column, you’ll see each module (Projects, Desks, Clients, etc.) along the left.
Click checkboxes to grant or revoke “View own” (only records they own) and “View all” (every record) rights.
For nested modules (e.g., under Clients: Export, Import), expand the section to expose sub-permissions.

7. Modify Manage Permissions
In the **Manage** column, toggle “Manage own” and “Manage all” to allow editing, creating, or deleting records.
Some modules also offer special rights such as “Send a private message” under Clients.

8. Add or Remove Specific Actions
Beyond the view/manage dichotomy, certain modules include granular options:

1. Under **Employees**, you might toggle “Create/Edit” vs. “Delete.”
2. Under **Settings**, you can enable or disable access to languages or verification levels.

9. Save or Cancel Changes
Once you’ve made your adjustments, click **Save** to apply them immediately.
To abandon your edits, click the back arrow or **Cancel**—no changes will be saved.
Here, you can delete permissions set during the role creation stage or add new ones. You can also set or change a template for the role.

> **Note**: For roles created or edited based on templates, you can only change the templates later, but not edit the permissions manually.

The **Edit Role** feature lets you keep your permission structures up-to-date as your team grows and business processes change. By carefully balancing view and manage permissions—optionally leveraging templates for common job functions—you maintain tight security controls while empowering employees with exactly the access they need.

Permission Enforcement Across Modules

Role permissions are not cosmetic or UI-based restrictions.
They are enforced at the backend level and determine which records are returned by the system.

For modules that depend on hierarchical access control (such as Clients, Leads, Orders, Requests, etc.), visibility rules are evaluated using the combination of:

1. Project permissions (View own / View all)
2. Desk permissions (View own / View all)
3. Client permissions (View own / View all)

Records are returned only if they pass all applicable permission checks.

This means:

1. If a role has **Project → View own**, only records from assigned projects are accessible.
2. If a role has **Desk → View own**, only records from assigned desks are accessible.
3. If a role has **Client → View own**, only records where the manager is assigned to the client are accessible.

Modules do not rely on frontend hiding.
Permissions are enforced server-side and define the actual data scope.

Revision #11
Created 4 September 2024 10:13:46
Updated 20 May 2026 13:08:29 by Anastasiia Rudaya