User Authorization

Module Guide: User Authorization

Module Location

Settings > Function Authorization > User Authorization

Module Purpose

The **User Authorization** module is the system's security control center, where the Administrator defines "roles" or "functional positions" in the form of **Authorization Groups**. Each of these groups represents a collection of access rights to various menus, buttons, and functions throughout the system. This is the core of the **Role-Based Access Control (RBAC)** mechanism, which determines "who can do what".?

1. Main View (List of Authorization Groups)

The main page displays a list of all roles or authorization groups that have been created.

View Explanation

- **Filter**: Allows searching for a group by **Group ID**.
- **Add Group**: A link to create a new authorization group.
- **Group Table**:
  - **Group ID**: A unique ID for each group.

- **Group Name**: The name of the functional role (e.g., `1_MANAGING_DIRECTOR`, `2_MANAGER_ACCOUNTING`).
- **Description**: A brief explanation of the group's role.
- **Status**: Indicates whether the group is active (Aktif) or not.
- **Action**: Clicking on a row will take the user to the **Change** page to manage that group.

2. Change Page (Authorization Group Details)

This page is the form for editing the details of a group and serves as the gateway to setting its specific access rights.

View Explanation

- **Basic Information**:
  - **Group Name & Description**: Fields to change the name and description of the role.
  - **Status**: An "Active" checkbox to enable/disable the group.
- **Advanced Action Buttons**:
  - **Change**: Saves changes to the name, description, or status.
  - **Admin Group**: Likely used to designate which users can manage the membership of this group.

- **User Authorization**: This is the most important button. Clicking it will most likely open a security matrix page, where the administrator can check off every menu, sub-menu, and function (e.g., Create, Change, Delete) that this group is allowed to access.

- **Delete**: To delete the authorization group.

3. Steps to Set Access Rights

- **Create New Group**: From the main page, click **Add Group**, give it a name and description (e.g., "Purchasing Staff"), and then save it.

- **Set Access Rights**: Click on the newly created group, then click the **User Authorization** button.

- **Assign Permissions**: On the security matrix page that appears (not shown), check all the menus and functions that the "Purchasing Staff" are allowed to access (e.g., can 'view' and 'create' a `Purchase Requisition`, but cannot 'delete' a `Purchase Order`). Save that permission matrix.?

- **Assign Users to Group**: Finally, go to the **Employee Data** module, find the relevant employee, and in the "Function Authorization" section, add the employee to the "Purchasing Staff" group.

4. Integrated Workflow & Business Process

- **RBAC Implementation**: The workflow above is a full implementation of **Role-Based Access Control**. Access rights are not granted to individuals, but to roles (groups). Individuals are then assigned to those roles.?

- **Dynamic Security**: When an employee ("Purchasing Staff") logs in, the system checks their group. The system will then only display the menus and enable the buttons that have been permitted for that group in this module. All other functions will be hidden or disabled.

- **Security Hub**: This module, along with **Employee Data**, is the center of the entire system security framework. The settings here define the boundaries of authority for every user across the entire application.

5. Tips & Important Notes

- The group structure should be carefully designed to reflect the actual functional roles in the company. Avoid creating too many overlapping groups.

- Apply the **Principle of Least Privilege**: Always grant the minimum access rights necessary for a role to perform its duties.?

- The "User Authorization" button leads to the most sensitive area. A configuration error here can grant excessive access rights or, conversely, prevent users from doing their jobs.

- Managing this module is the exclusive task of the System Administrator or an equivalent role fully responsible for application security.

Revision #1
Created 23 October 2025 08:17:16 by Sayu
Updated 23 October 2025 08:18:37 by Sayu