User Defined Report Settings

Module Guide: User-Defined Report Settings

Module Location

Settings > Reports > User-Defined Report Settings

Module Purpose

This module serves as a control panel for setting up role-based or position-based access rights to specific reports. Its purpose is to ensure that reports containing sensitive or relevant data can only be accessed by users with appropriate job positions, such as managers or higher-level staff.

View and Feature Explanation

The main page of this module displays a list of reports for which access has been specifically configured.

Search Filter:

- **Report Name**: Allows an administrator to search for the access settings of a specific report.
- **Search**: A button to apply the filter.
- **Show all**: Clears the filter and displays all settings.

Settings List Table:

- **Report Name**: The name of the report for which access is being configured (e.g., `Campaign Report`).
- **Allowed Positions**: Shows the names of the positions or job titles that have been granted the right to access the report (e.g., `GENERAL MANAGER`).

Action Buttons:

- There are likely "Add New" buttons to create new access rules and "Delete" buttons to remove existing rules, although they are not actively shown in the image.

Expected Workflow (Based on Convention)

1. **Creating a New Rule**: The administrator opens a new form to create an access rule.
2. **Selecting a Report**: The administrator selects one report from the list of all existing reports in the system.
3. **Defining Positions**: The administrator selects one or more job positions (e.g., Sales Manager, Finance Director, Warehouse Manager) that are allowed to view the report.
4. **Saving the Rule**: Once saved, only users who hold the specified job positions will see and be able to open the report from their report menu.

Integrated Workflow and Business Process

- **Data Access Control**: This is a very important data security function. A company can limit access to sensitive financial reports to only the board of directors, or restrict sales performance reports to only the sales team and their managers.

- **Information Confidentiality**: Prevents staff from one department from viewing the performance data or sensitive data of another department, maintaining confidentiality and the work focus of each team.

- **Simplified View**: By limiting the reports that are visible, the report menu for each user becomes simpler and contains only the reports that are relevant to them, making it easier to use.

- **Compliance**: For industries that are strictly regulated, controlling access to data and reports is one of the compliance requirements that must be met.

Tips and Important Notes

- **Job Structure**: The effectiveness of this module is highly dependent on how the job or position structure is defined within the system (usually in the HR or User Management module). Ensure that the structure is accurate and up-to-date.

- **Principle of Least Privilege**: Apply the principle of minimum access rights. Grant access to a report only to positions that truly need it for their work. Always start with the least privilege and add more only if it is absolutely necessary.

- **Custom Reports**: If the company creates new custom reports, do not forget to set their access rights through this module if the reports contain sensitive data.

Revision #1
Created 23 October 2025 14:34:18 by Muhammad Ali Akbar
Updated 23 October 2025 14:35:34 by Muhammad Ali Akbar