

Function Authorization Report

Module Guide: Function Authorization Report

Module Location

Settings > Function Authorization > Function Authorization Report

Module Purpose

The **Function Authorization Report** module serves as an audit and access verification tool. It allows an administrator or manager to see the exact, complete list of all functions, menus, and permissions (e.g., `read`, `write`, `delete`) held by a user or a group of users. It is the way to answer the question, "What can user X actually do in the system?"

1. Main View (Report Generator)

The main page is an interactive interface for selecting users and generating their access rights report.

View Explanation

- **User List:** A box on the left containing a list of all active users in the system.
- **Selected User:** A box on the right containing the list of users who have been selected for reporting.
- **Movement Buttons:**

- **>>**: Moves a user from the "User List" to the "Selected User" box.
- **<<**: Removes a user from the "Selected User" box.

- **Action Buttons:**

- **Show Report**: Generates a printer-ready access rights report for all users in the "Selected User" box.
- **View via Excel**: Exports the detailed access rights of the selected users to an Excel file.

2. Access Rights Report View

After users are selected and the "Show Report" button is clicked, the system generates a detailed report in a pop-up window.

View Explanation

- **Report Header**: Displays the company name and the information of the user whose report is being shown (e.g., A. Bagus Nur Sudrajat).
- **List of Access Rights**:
 - This report presents a complete list of all functions and modules accessible to that user, organized by main menu (e.g., General Ledger, Purchase, Finance, Inventory).
 - For each function, the report details the level of permission held, such as (read), (write), or (delete). This provides a very granular view of the user's authority.

3. Steps to Create a Report

- Access the **Function Authorization Report** module.
- In the left box ("User List"), select one or more users whose access rights you want to check.
- Click the >> button to move them to the "Selected User" box.
- Click the **Show Report** button to view the report in a printable format or click **View via Excel** for further data analysis.

4. Integrated Workflow & Business Process

- **Verification and Audit Tool:** This module is crucial for the security audit process. Auditors (both internal and external) can use this report to verify whether the implementation of access rights in the system complies with the company's **Segregation of Duties (SoD)** policy.
- **Access Troubleshooting:** If a user reports that they cannot access a certain function that should be part of their job, an administrator can quickly run this report to see what access rights the user actually has and identify the problem (e.g., the user has not been assigned to the correct authorization group).
- **Security Documentation:** The generated report can be saved as official documentation of the user access rights matrix at a specific point in time, which is useful for compliance and record-keeping purposes.

5. Tips & Important Notes

- Use this report proactively, not just reactively. Schedule a periodic review of access rights reports (e.g., monthly or quarterly) for all users, especially those in sensitive roles.
- Compare the reports of several users who should have the same role to ensure consistency in access rights.
- Because this report contains highly sensitive security information, access to the **Function Authorization Report** module itself must be strictly limited to System Administrators, IT managers, and the Internal Audit team.

Revision #1

Created 23 October 2025 08:19:12 by Sayu

Updated 23 October 2025 08:21:03 by Sayu