# System Log

## Module Guide: System Log (User Login Logout)

### Module Location

Settings > System Settings > System Log

### Module Purpose

The **System Log** module serves as a security audit trail that records all user login and logout activities within the system. Its purpose is to provide a clear digital footprint of who accessed the system, when they logged in and out, and where they accessed it from. This is a crucial tool for security monitoring and user activity analysis.

## View and Feature Explanation

The main page of this module is the interface for viewing and filtering log data.

## Search Filter

- **User ID**: Allows an administrator to filter the log and display only the activities of a specific user.
- **Start Date** and **End Date**: A time range filter to view login or logout activities within a specific period.

- **Search**: A button to apply the selected filters.
- **Show all**: A button to clear all filters and display the entire log record again.

## Log List Table

- **No**: Serial number.
- **User ID**: The unique ID of the user who performed the activity.
- **Employee ID**: The employee ID associated with the user account.
- **User Name**: The name of the user account.
- **Employee Name**: The full name of the employee.
- **IP Address**: The IP address from which the user logged in.
- **Log Date**: The exact date and time when the login or logout activity occurred.
- **Time(ms)**: Most likely records the session duration or system response time in milliseconds.

## Action Buttons

- **Delete**: A button to delete the selected log records. This action should be performed with extreme caution.

# Integrated Workflow and Business Process

- **Security Auditing**: The primary function of this module is for security audits. Administrators can regularly review the logs to detect suspicious activities, such as login attempts from unknown IP addresses or activities outside of normal working hours.

- **User Activity Monitoring**: Helps in monitoring user compliance with company policies. For example, to ensure users log out at the end of the workday.

- **Incident Investigation**: If a security incident or data error occurs, the System Log is a crucial starting point for an investigation. An administrator can track who was active on the system at the time of the event to narrow down the possible causes.

- **System Performance Analysis**: The `Time(ms)` column can provide initial insights into the system's performance and response speed during user interactions. Consistently high times may indicate a performance issue.

# Tips and Important Notes

- **Log Retention Policy**: The company should have a clear policy on how long this log data is to be stored. Deleting logs too quickly can hinder investigations, while storing them for too long can overload the database.

- **IP Address Security**: Pay attention to unusual IP addresses. If your company uses an internal network, all logins should originate from an internal IP range. Logins from unexpected

external IPs should be investigated immediately.

- **Delete Action**: Deleting log records should be restricted and strictly regulated. In many compliance standards, deleting audit logs without a clear reason is a serious violation.

---

Revision #1
Created 23 October 2025 14:25:19 by Sayu
Updated 23 October 2025 14:26:39 by Sayu