Activity Logs Setup

Activity logs maintain a record of any specified statistics of system usage, which can assist with auditing your system. You can view current activity logs in the Activity Logs table.

It's often useful to create rules based on the events you track. For instance, you could create a rule to notify you when someone changes a workflow, rule, or user record. You can also set up reports for activities that pose a security concern. For instance, you could create a report for failed logins that alerts you regarding potential attempts to breach the login screen.

> ⚠ To access the Activity Logs table, go to **Setup > Tables**, select Activity Log, and click Unhide. From there, you can use the nav bar menu icon to search for it, or add it to your navigation menu (**User Menu > Preferences > Navigation Menu Setup**).

Configuring Activity Logs

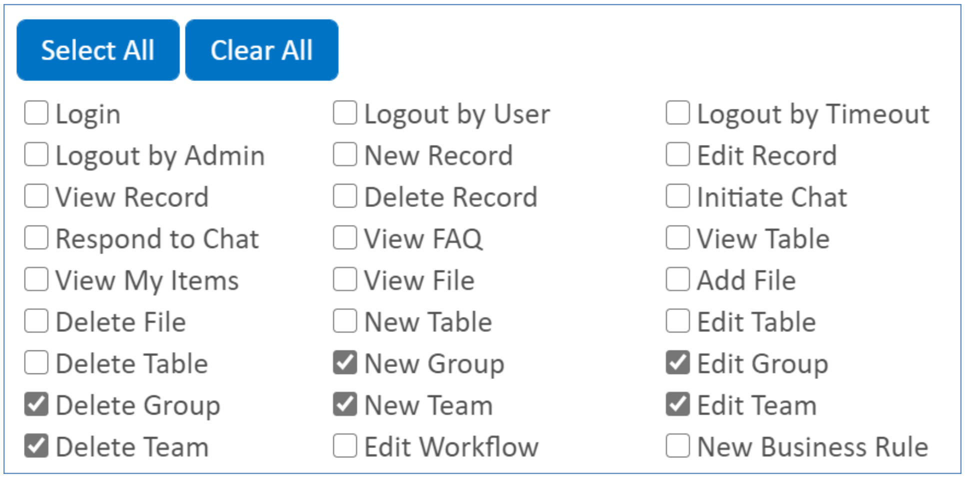
You can configure your activity logs by creating different audit rules. Audit rules define which system activity is tracked and how long activity logs are maintained. To view existing audit rules, go to **Setup > System > Configure Activity Log**. You can create new audit rules by clicking New to open the Audit Rules wizard.

The Audit Rules wizard is a single screen that allows you to choose to track various system events and create saved searches that determine which users' actions are logged. Many different kinds of events can be tracked: login failures, action bar edits, record views, and others. The system creates records in the Activity Log table when the events you select meet the saved search criteria.

To create an audit rule:

1. Click the **Setup** gear in the top-right corner and go to **System > Configure Activity Log**.
2. Click New to open the Audit Rules wizard.
3. Name the audit rule and select a language for the audit report.
4. Create or select a saved search that determines which users actions are logged.

5. Select which events are logged for the users meeting the saved search criteria. An event is only logged if it selected from this list and is executed by a user who meets the saved search criteria. For example, you might want to only log specific actions from admin users, such as when they edit a team or group.



☐ Login
☐ Logout by User
☐ Logout by Timeout
☐ Logout by Admin
☐ New Record
☐ Edit Record
☐ View Record
☐ Delete Record
☐ Initiate Chat
☐ Respond to Chat
☐ View FAQ
☐ View Table
☐ View My Items
☐ View File
☐ Add File
☐ Delete File
☐ New Table
☐ Edit Table
☐ Delete Table
☑ New Group
☑ Edit Group
☑ Delete Group
☑ New Team
☑ Edit Team
☑ Delete Team
☐ Edit Workflow
☐ New Business Rule

Example with group and team creation, editing, and deletion selected

6. Define for how long the system retains entries created by the audit rule. If an audit rule is deleted, any records created by the rule are also deleted.
7. Click Finish.

Log files generated from activity logs and other system activity are deleted with the Logeraser utility. By default, log files are deleted after 30 days. To change Logeraser's default settings, you must have access to the file directory on the server.