

Sage Line 500 - Auditing and Security

This module provides functionality to audit events such as the addition of new master records or the update of critical fields and to limit access to data for specific users.

The security options are only available on database systems.

Records Kept

Audit notes

- Define reason codes to be recorded when the following types of event take place:
 - Addition of a new record.
 - Update of existing data.
 - Deletion of a record.
 - Deletion of a batch of items.

Audit events

- For each audited event, record data from the record being affected plus the date, time, user who made the update and the event type.

Security user groups

- Assign users to groups to simplify set up and maintenance.

Secured tables

- List which tables may be secured through which options. A list is provided as part of the standard system. Modules covered are:
 - General Ledger.
 - Accounts Receivable.
 - Accounts Payable.
 - Project Ledger and Resource Ledger.
 - Invoicing and Sales Analysis.
 - Purchase Order Processing.
- Record a link between a specific table and column combination to one with secured ranges applied.

Security details

- Record update, enquiry and reporting access rules for tables.

Tasks Supported

Maintain auditable tables

- Update the list of tables that may be audited.

Maintain audit rules

- Specify which events are to be audited. Types of event are addition, update, deletion and batch deletion. For instance, you can audit all additions and deletions to the Fixed Asset register.

- For each event:
 - Specify the level of auditing required, for instance require that whole row be saved, individual column values saved, or just record the event.
 - Specify the name of the column whose value change triggers audit.
 - Specify an audit note type to force a reason to be recorded.
- Enable overrides to credit stop to be audited as a special event.

Maintain secured tables

- View the supplied active secured tables.
- Add security to tables.
- Remove security from tables.
- Specify ranges of data in character type columns to be restricted.

Maintain security details

- Define, either by user or user group, exactly which records may be updated, enquired upon, or reported upon. For example, if you have selected the table and option combination of purchase_supplier and purchase_invoice, and have selected supplier ranges of A001-B001 for users in group 01, those users will not have access to any purchase invoices from suppliers that fall within those ranges.

Reporting

Audit enquiries

- Audit Enquiry By Table, for instance enquire on customer master file events.
- Audit Enquiry By Event, for instance enquire on credit limit updates on the customer file.
- Archive Enquiry. Enquire on archive events for those archiving routines that have been enabled for auditing.

Audit reporting

- Audit Report. Report events, selecting by table, range of users, event type and date range.

Housekeeping

- Clear down audit details for all tables or a specified table based on a userdefined cut-off date.
- Load the security monitor into shared memory for optimum software performance.

Integration with other modules

Report Writer

- Design your own reports on audited events.
- Reports designed using the Report Writer module follow the security access rules defined.