Security

A transparent layered security model provides the foundation for the Tencia user experience. It aims to deliver a user experience which helps both employees and systems administrators become more efficient and productive.

Tencia's security features include:

- Security based on roles. Tencia groups individual users that have similar characteristics into 'roles'. A role could be based on job function, e.g. customer order entry and processing or on position e.g. senior management.
- Tencia incorporates code level permissions, which is a facility to assign a permission level on predefined system codes such as debtor, creditor or stock codes. This limits the type of data that can be accessed by users and ensures sensitive details are not easily accessible.
- User defaults can also be set which means that some fields in a data entry screen can be by-passed based on the user default that has been applied to these fields. Information is therefore pre-populated into these fields which means they can be by-passed so that data entry is streamlined which also minimises errors during data entry.
- Security levels can be applied to individual menu programs. A security level of 1-9 with 9 representing the highest level can be applied which will determine which programs are displayed in the users menu.