Retain Security Manual

Table of Contents

1 Introduction 3
1.1 About Retain 3
1.2 About Retain Security 3
1.3 What's new 4
1.4 About this guide 4
1.5 Where to get support 4
1.6 Installing Retain 4
1.7 Conventions 4
2 General principles 5
2.1 Introduction 5
2.2 Thinking it through 5
2.3 Preparing your data 5
3 Starting Retain Security 6
3.1 Overview 6
3.2 Getting started 6
3.3 The Retain Security interface 7
3.4 Save and Exit Retain Security 7
4 Security 8
4.1 Overview 8
4.2 Roles 8
Set up Roles 8
Row level Access 9
Functional Access 11
Functional Access Values 12
4.3 User Security 18
User security settings 18
Licence settings 20
5 Tables 21
5.1 Database table alias and default options 21
5.2 AND, OR (Closed) and OR (Open) Security 23
5.3 Field display order 23
6 Database 25
6.1 Database settings 25
7 Calculated Fields 26
7.1 Changing the description 26
8 Appendix 27
8.1 Additional components 27
9 Support 28
9.1 Support services 28
Index 29

1 Introduction

Retain Security Manual

www.retaininternational.com

1.1 About Retain

Retain is a flexible planning tool for viewing and manipulating staff and job allocations through a user friendly graphical interface. It has been designed to resemble the manual "wallchart" booking system, but it is much more versatile than any manual booking system.

1.2 About Retain Security

Retain Security is an administration tool for Retain. It is used for initial setup and the subsequent administration of Retain users and some data files.

Retain Security is used to define and maintain:

- user roles
- user security
- field properties (Tables)
- database settings
- calculated fields

1.3 What's new

Retain 4 offers a few new technical features, that make Retain Security more powerful. For example,

- Enhanced flexibility with user access security. You do not have to set up security for individual users. This means that you can assign security for one user, against many resources. You assign the relevant user within Retain.
- Ability to change field properties including field order in Retain Security.

1.4 About this guide

Refer to this guide if you are doing any of the following:

- Set Retain up for the first time
- Perform administration tasks

Refer to the Retain help file for making bookings, viewing staff plans or reports.

1.5 Where to get support

If you have a problem with Retain products that you are unable to resolve through this user guide or through your local support contacts, please contact your Support Service Provider.

1.6 Installing Retain

See Technical Implementation guide for further details.

If you are involved in the initial setup using Retain Security, the chapter on General Principles gives a rough idea on what need to be thought through.

After installation, Retain Security is enabled for full functional access for a limited number of attempts to allow the initial setup of the access permissions.

1.7 Conventions

The following conventions are used throughout this user guide:

- Menu options and options within dialog boxes are expressed in single quotes, for example:
  Select 'Data', 'Edit' from the menus.
- Keyboard strokes are represented by capitals, for example:
  ENTER represents the Enter or carriage return key (also referred to as the RETURN key in some computer manuals).
  ESC represents the Escape key.
  F1, F2 etc., represent the function keys.
  SHIFT represents the Shift key.
  CTRL represents the Control key.
  ALT represents the Alt key.
- A plus sign between two key presses indicates a combination of key presses, for example CTRL+S represents the action of holding down the Control key and pressing the S key.

2 General principles

2.1 Introduction

This chapter contains information of vital importance to the initial setup of Retain. Most users will not need to read this chapter.

Thinking it through gives some ideas about how to approach the security options and achieve a clear, consistent and simple set of conventions.

Preparing your data gives the data backdrop against which the security options will have to exist, so that the structures are as harmonious as possible.

2.2 Thinking it through

It is important to think through the way in which you would like options to be set up in Retain Security. Starting in an ad-hoc fashion will result in confusing roles, users and defaults. This topic gives some ideas on the user security settings. The topic on preparing your data gives some ideas for how to approach the database tables, their defaults, aliases and limited lists.

You will want to try to make the role names reflect your longer term aspirations. For example, you may decide to have a super administrator and several sub-group administrators. These could be grouped by geography, subject, department, letter, number, etc. There will also be function-based roles, such as view, edit own line, etc. Make sure you develop a convention which will make the system easy to maintain and intuitively obvious, and consider using several sub-groups to define a group rather than creating many different unique roles. For example, you could have several levels of user in an office. They could be identified by combinations of the office role, view role, edit own line role, and administrator role. Thus there would only be one role unique to the office, the other three roles being used generally in many other groups, including other office groups.

A similar clarity is needed for the role names for functional access.

For users, you do not need to enter every user as an individual. Many will simply use the 'Default' user. Note that names must be unique, so your naming convention for users needs to have a simple strategy for coping with identical names within the naming convention used.

2.3 Preparing your data

This topic gives the data backdrop against which the security options will have to exist, so that the structures are as harmonious as possible. Before using Retain on a daily basis, it is useful to set up permanent information, such as staff names and names of recurring tasks or assignments, so that this information will be readily available when you need to use it.

You should also think through the way in which you are going to structure your data files and then collect together the raw material in readiness for input. This process is likely to include:

- Defining conventions for the usage of the various fields in the Resource and Job data files.
- Preparing a schedule of staff and equipment details to add to the Resource data file.
- Preparing a schedule of recurring or forthcoming assignments to add to the Job data file.
- Preparing a schedule of generic sub-tasks to add to the 'Components' data file.

You may prefer to implement Retain starting with a blank database, allowing users to add records as and when they are needed. However, dealing with the set-up of data files as an 'up-front' exercise has several advantages:

- Conventions for usage of the different fields can be firmly established on set-up and are therefore less likely to be ignored.
- Data can be collated and checked centrally from other sources, such as staff and client systems, therefore reducing the risk of error.
- There may be scope to transfer this data automatically from other systems.
- People planning can see who is available and what assignments need to be planned from day 1.

3 Starting Retain Security

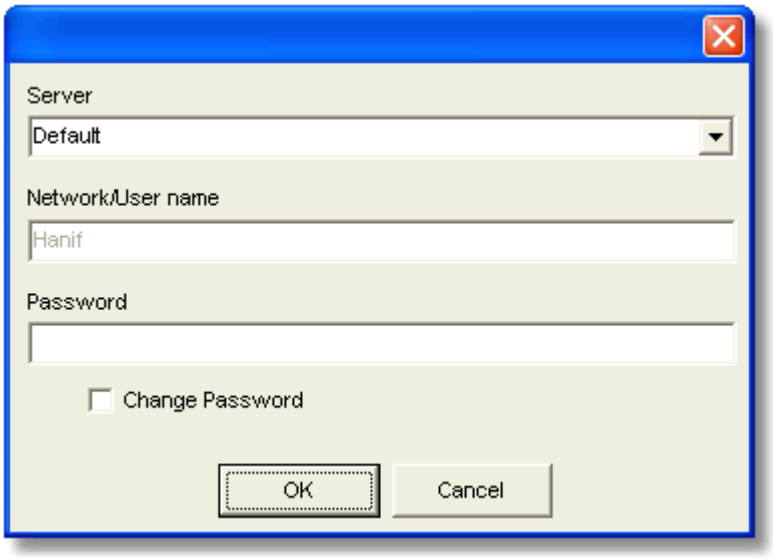
3.1 Overview

Retain Security is used for initial set-up and the subsequent administration of Retain users and data files. However the main purpose of Retain Security is to create users and set up their levels of access to Retain and to Retain Security itself.

To start Retain Security see Getting Started. To learn how to set up users and assign them roles see Users security settings. For other settings see Licence settings and Database settings for details.

3.2 Getting started

You should find Retain Security under the main Retain group from Start Menu. You may be prompted with a logon box:



Server

It is the Retain Server you are connecting to, which should be left as Default since initial installation. However if you have more than one server set up you can choose an alternative from the drop-down list.

Network/User name

It should be consistent with the user's Windows logon. However if you are opening Retain Security for the first time it will have a default value e.g. Administrator.

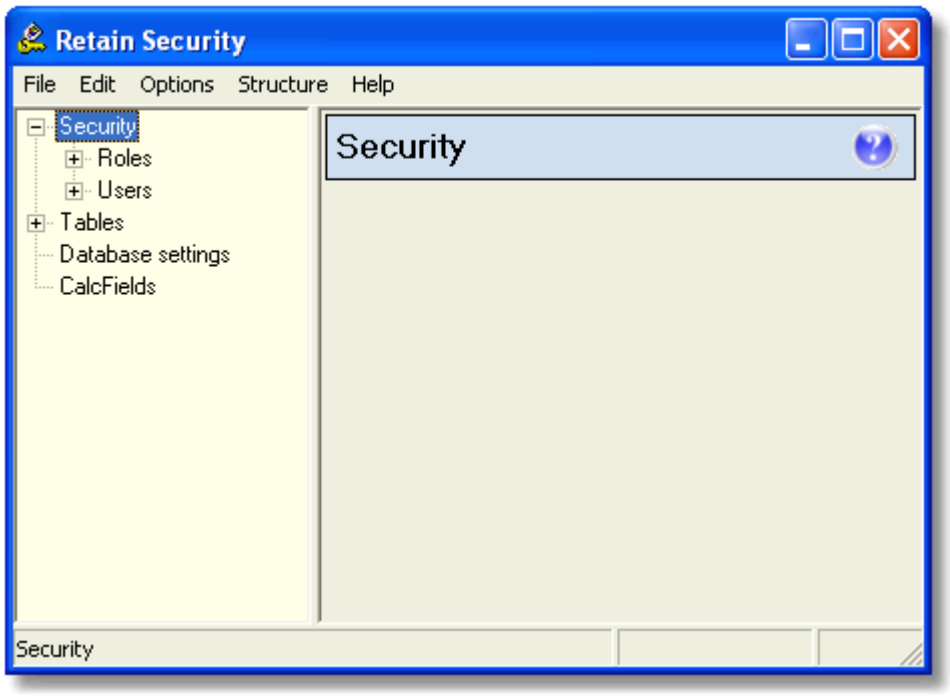
Password

It should always be left blank unless for special configuration setups.

Click OK to open Retain Security or Cancel to exit.

3.3 The Retain Security interface

The Retain Security user interface will have entries like the ones shown below:



Here you can maintain:

- user roles
- user security
- field properties (Tables)
- database settings
- calculated fields

3.4 Save and Exit Retain Security

After you edit each item in Retain Security, you should save the changes by clicking on **Save Changes** button shown below. You can use the **Undo Changes** button to reverse your last change.

To exit Retain Security choose 'File | Exit' from the menu, or click on the 'X' button at top right corner. You can also use shortcut ALT+F4.

If you exit without saving any changes made, Retain Security will automatically save the changes for you.

4 Security

4.1 Overview

The following options in Retain Security support the administration of users and access rights:

- *Roles* – defines access rights by field, row or function. Roles are then used in both group and user definitions to select appropriate access right.
- *Users* – defines the access rights for a user by making the link between the roles, and/or roles aggregated into groups, and the user.

4.2 Roles

Set up Roles

Roles are global access levels that are used when assigning specific access rights to users.

There are two **types** of roles, each defining roles from a different angle:

- Row level access – enables access permission for a "row" in a table where a condition can be based on.
- Functional access – enables access permission to perform specific functions in the modules of Retain.

The access permissions are **Read**, **Insert**, **Update** and **Delete.**

To create a new role:

- Right-click on the appropriate role type, e.g. 'Row Level Access' and choose 'Add' or click the  button.
- Enter a name for the new role and click 'OK' .

It is worth taking care to use different names in the different role types, otherwise you could have up to three items of the same name in your role list with no way to differentiate.

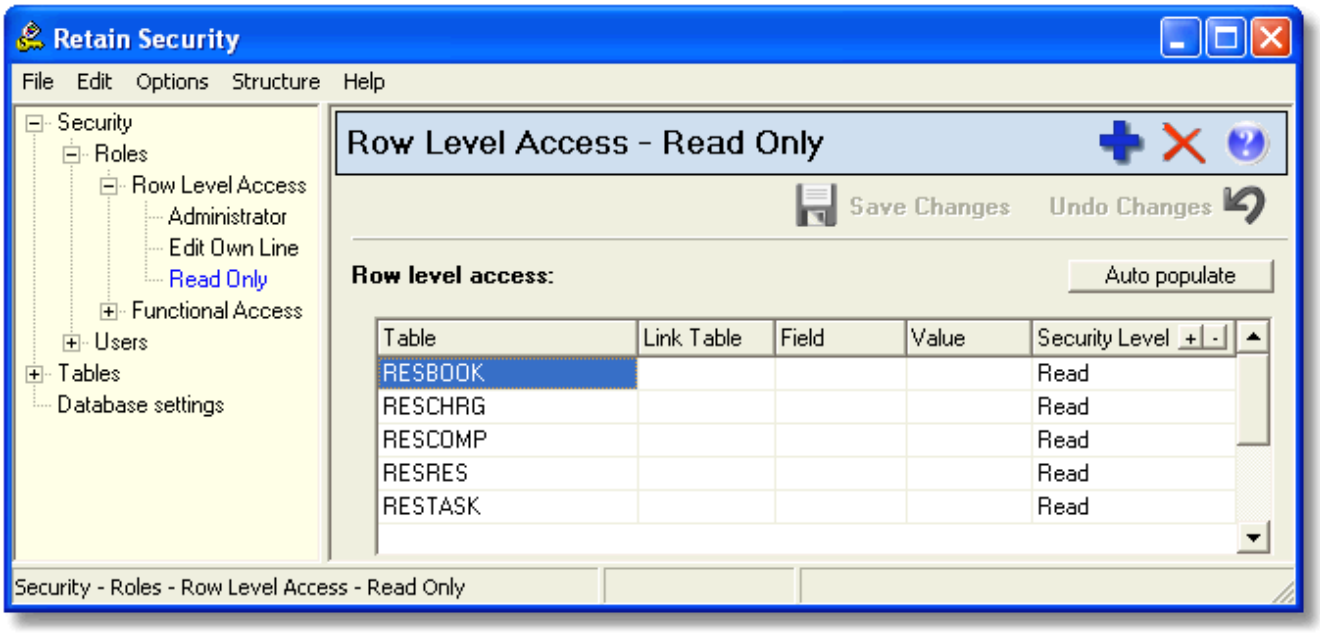
To rename an item, right-click on the item and select 'Rename'.

To remove an item, right-click on the item and select 'Delete'.

Retain will not run without the Default role settings. Do not delete or rename any default settings.

Row level Access

Row Level Access defines how a user can access the rows in a particular table.

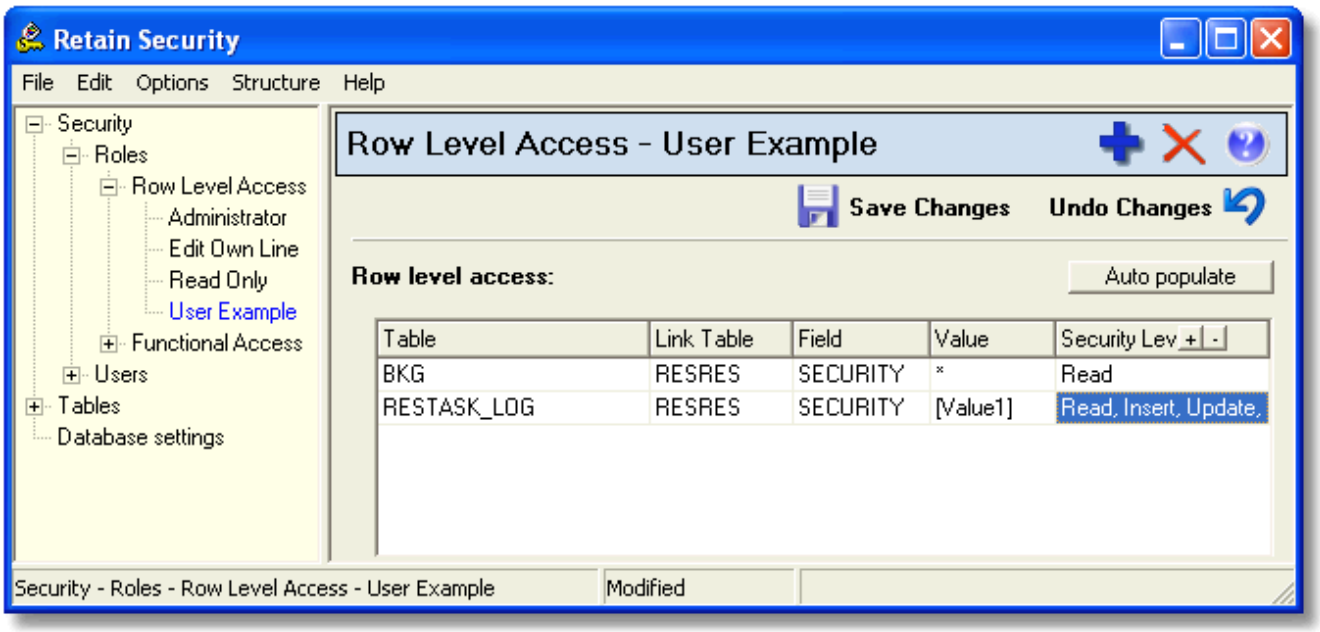


The default roles are:

- Read Only - view information only and independent on any field value
- Edit Own Line - full access permission to user's own bookings but view only access to others
- Administrator - full access permission to all information

To create a new role:

- Right-click on 'Row Level Access' in the left pane and choose Add or click on  button.
- Name the new role.
- To add a condition to the right pane click the + button or delete by clicking the - button, and define the role.

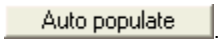


- *Table* – select the table in which the field resides.

- *Link Table* – select the table where the conditional field resides.
- *Field* – select the field upon which the condition is to be applied.
- *Value* – the value of the field on which the condition is set. Enter * as the value to imply 'any' value.
- *Security Level* – the permission(s) of access allowed to those selected rows.

The 'User Example' role defined above is a template where you can allow users with different security settings to access booking records. You can change [Value1] to identify the administrator users who can have full access rights to the booking records in BKG table. All the other users will have read only access.

Rather than starting from scratch you may want to create a new role that is similar to or based on an existing role by 'Auto populating':

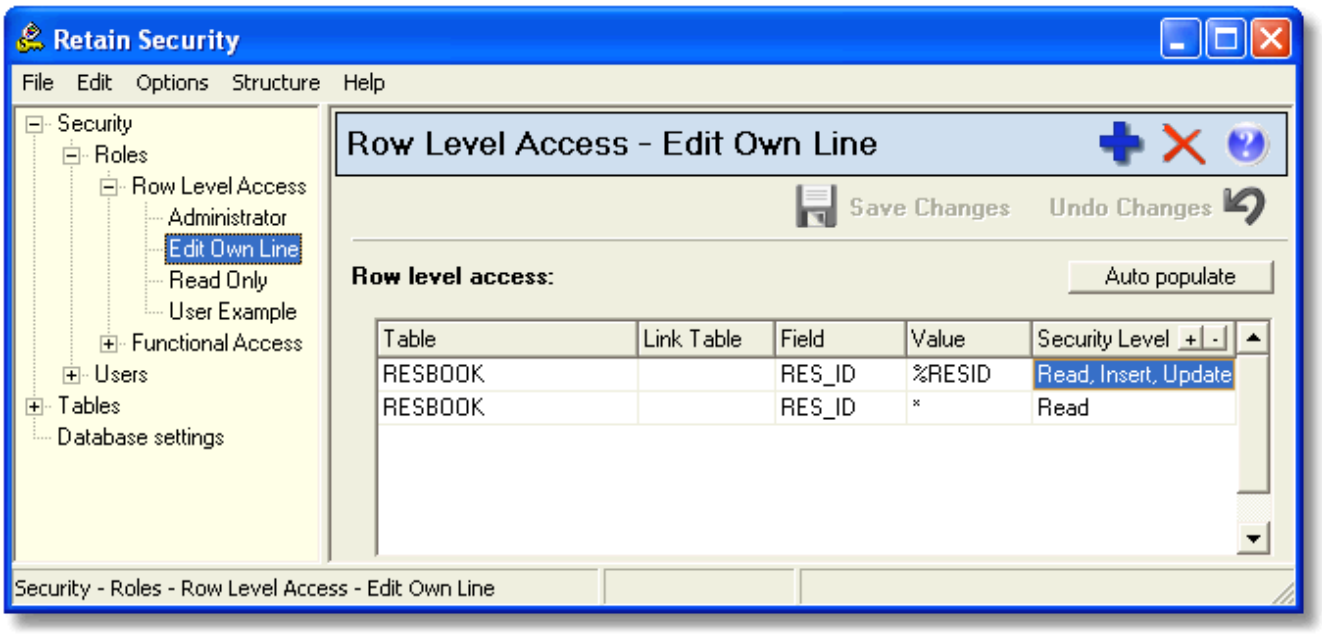
- Click on the Auto populate button in the right pane 

.
- Pick a suitable existing role from the list.
- Click on the OK button.

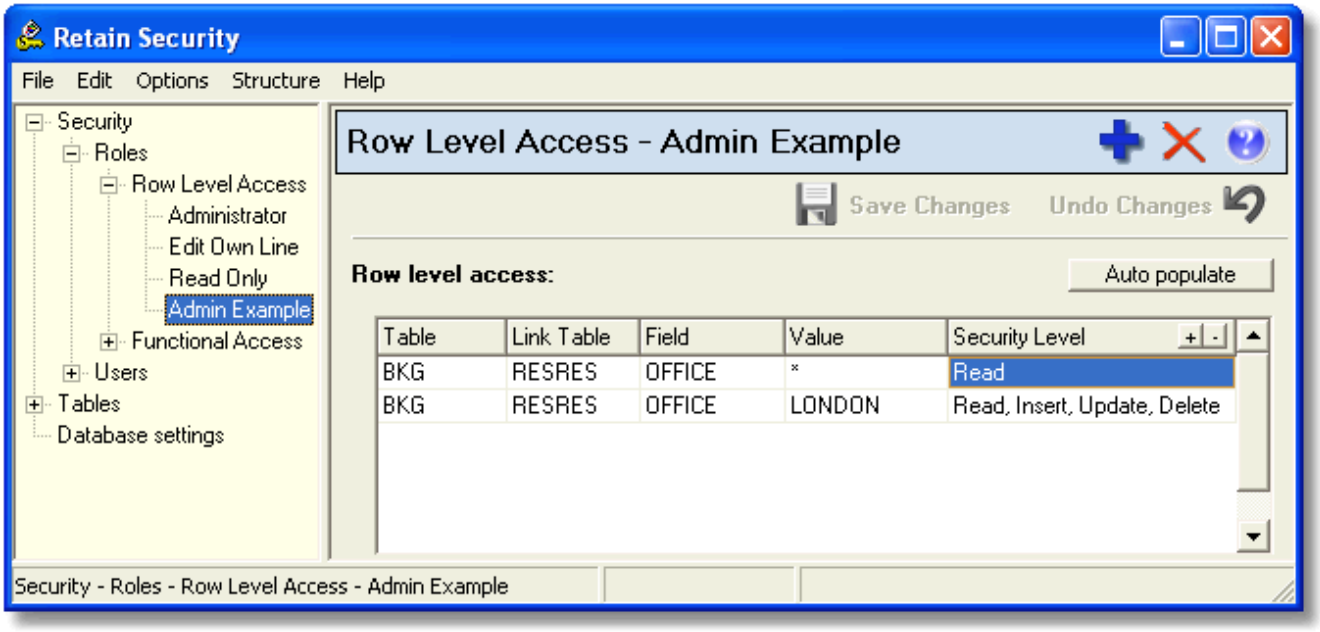
This will populate the new role with the access rights of the selected role. You can then edit on top of this role.

For users who will be allowed to edit their own bookings, the role 'Edit Own Line' is set up.

> Note the use of %RESID to match the ID of the resource with the ID of the booking so that only the resource with matched ID can have full access to their bookings.



You can define roles to suit your organisation's requirements. For example, you may have offices in different locations and the access rights need to be different.



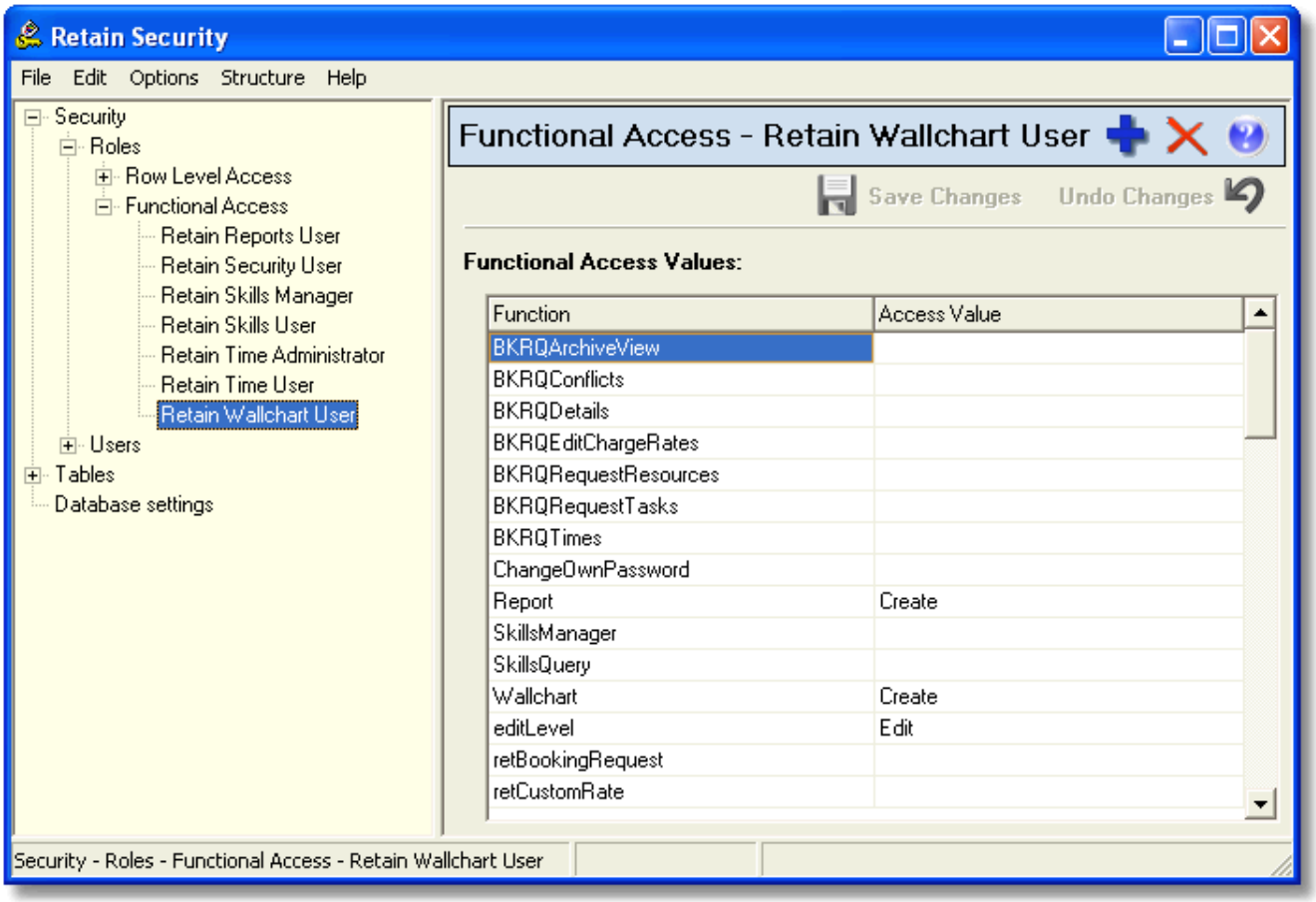
The role shown in the example above defines that administrators in the London office can have full access to the BKG table otherwise they have read only access.

Notes:

- Security access can be based on any field in the database, with any value. You can determine what data users actually see by the tables and associated field values you specify.
- Multiple fields and values can be used in defining roles, for example a second location value can be added which will then show those resources and bookings where the office field has a value of London or Paris.

Functional Access

Functional Access defines what function modules of Retain Resource Planning System a user can access.



The default functional access roles are:

- Retain Reports User - full access to Enterprise Reports module.
- Retain Security User - full access to Retain Security.
- Retain Skills Manager - full access to Retain Skills Manager module.
- Retain Skills User - ability to search for users with specific skills in Retain Skills Selection module. No access to Retain Skills Manager module.
- Retain Time Administrator - full access to Retain Time module.
- Retain Time User - enter timesheet information in Retain Time module. Must specify a 'Resource' against the user.
- Retain Wallchart User - permits access to Retain. Use this in conjunction with a Row Level Access role to grant different levels of access.

The list below shows a naming convention used for the functions listed in the right pane.

- BKRQ Booking Request
- ret Retain
- rrp Enterprise Reports
- rsm Retain Security
- Skills Retain Skills
- time Retain Time

The various permissions, or functional access values, are generally obvious from the title of the function and the drop-down access value list. For example, BKRQArchiveView specifies whether the user of Booking Request is allowed to look at the whole archive (All), or the part of the archive relating to them only (Self), or has no access to the archive (None). You can define your own functional access roles according to your needs, for example you can define a 'Full Function' role that has all the functions.

Notes:

- A higher level of access will override a lower one. If the Retain Security access is set to all functions i.e. rsmApplication = All then the subsidiary functions in Retain Security do not need to be defined and are left blank. If you assigned rsmApplication = Part, then you need to specifically select the level of access required for all the rsm functions.

Functional Access Values

The functions for each module:

Booking Requests
Retain Skills
Retain Wallchart
Enterprise Reports
Retain Security
Retain Time
Miscellaneous

Booking Requests

- **BKRQAdministerRequests** - Ability to see submitted requests and be able to reject them, make live or ghost. In the Booking Requests module it determines whether the Admin tab is visible, while in Wallchart it determines if the administration actions are available.
  - No
  - Yes
- **BKRQArchiveView** - Ability to see inactive booking requests (either live, logged or rejected) in the booking request module.
  - None - The archive tab is not shown.

- Self - The archive tab is shown but searches can be only performed on booking requests originated by the user.
- All - The archive tab is shown and searches are open (subject to row and logical security).

- **BKRQConflicts** - Whether the user can make booking requests which, if lived, would create a conflict.
  - No
  - Yes

- **BKRQDetails** - Whether the user can open the detailed view of a booking request.
  - No
  - Yes

- **BKRQEditChargeRates** - Whether the user can edit the charge rates of booking lines in the booking requests.
  - None - No ability to see or edit charge rates of the booking request lines.
  - View - Read only access to the charge rate information.
  - Write - Ability to read and edit the charge rates.

- **BKRQEditLoading** - Ability to edit the loading of booking request lines.
  - No
  - Yes

- **BKRQRequestResources** - Ability to submit booking requests for the user him/herself or multiple resources. In the booking request module it determines whether the user is able to see the User tab; in Wallchart it determines if the user has the ability of submitting booking requests.
  - None - No ability to perform booking requests.
  - Self - Request self in booking requests.
  - All - Request self or others in booking requests.

- **BKRQRequestTasks** - Whether the user is able to submit booking requests. The extensiveness of this functionality is partly determined by the BKRQRequestResources functional access.
  - No
  - Yes

- **BKRQTimes -** Currently not in use.
  - None
  - View
  - Edit

Retain Skills

- **SkillsManager** - Whether the user can run skillmng32.exe
  - None - No ability to run the executable.
  - Full - Ability to run the executable.

- **SkillsQuery** - Whether the user can run skillsel.exe.
  - None - No ability to run the executable.
  - Full - Ability to run the executable.

Retain Wallchart

- **retBookingRequest** - Whether the user is able to see and make booking requests.
  - No - No ability to see or make booking requests.
  - Yes - Ability to see and make booking requests.

- **retCustomRate** - Whether the user is able to see the cost tab in the make booking dialog.
  - No
  - Yes

- **retGhostBookings** - Whether the user is able to see or edit ghost bookings.
  - None - No ability to see or edit ghost bookings.
  - View - Ability to see ghost bookings only.
  - Edit - Ability to edit ghost bookings.

- **retRollForward** - Whether the user is able to use the roll forward functionality.
  - No
  - Yes

- **retTeamView** - Currently not in use.
  - No
  - Yes

- **retUserLevel** - Whether the user is able to view or edit records.
  - viewOnly - Ability to view records only.
  - fullViewer - Ability to create and edit report, calendar and wallchart pages but not manipulate records.
  - power - Ability to edit all records.

Enterprise Reports

- **rrpConsolidation** - Whether the user is able to report across multiple databases. Should be set to 'No' unless instructed otherwise.
  - No
  - Yes

- **rrpGeneral** - Whether the user has general access to Enterprise Reports. Should normally be set to the same value as rrpReports functional access.
  - None - No ability to access Enterprise Reports.
  - View - Ability to view Enterprise Reports only.
  - Edit - Ability to edit Enterprise Reports.

- **rrpReports** - Whether the user has access to individual reports. Should normally be set to the same value as rrpGeneral functional access.
  - None - No ability to access individual reports.
  - View - Ability to view individual reports only.
  - Edit - Ability to edit individual reports.

Retain Security

- **rsmApplication** - Whether the user is able to access Retain Security.
  - None -No ability to access Retain Security.
  - Part - Ability to access some parts of Retain Security, defined by other functional access values (listed below).
  - All - Ability to access Retain Security no matter what the other settings are.

- **rsmChargeRate** - Whether the user is able to edit charge rates.
  - None - No ability to edit charge rates.
  - Edit - Ability to edit existing charge rates.
  - AddRemove - Ability to add or remove charge rate categories.

- **rsmColorScheme** - Whether the user is able to edit colour schemes.
  - None - No ability to edit colour schemes.
  - Edit - Ability to edit existing colour schemes.
  - AddRemove - Ability to add or remove colour schemes.

- **rsmCurrency** - Whether the user is able to edit currencies.
  - None - No ability to edit currencies.
  - Edit - Ability to edit currencies.

- **rsmDBSettings** - Whether the user is able to edit database settings.
  - No
  - Yes

- **rsmDay** - Whether the user is able to edit settings for days.
  - None - No ability to edit settings for days.
  - Edit - Ability to edit existing settings for days.
  - AddRemove - Ability to add or remove day types.

- **rsmWeek** - Whether the user is able to edit settings for weeks.
  - None - No ability to edit settings for weeks.
  - Edit - Ability to edit existing settings for weeks.
  - AddRemove - Ability to add or remove week types.

- **rsmDiary** - Whether the user is able to edit diaries.
  - None - No ability to edit diary settings.
  - Edit - Ability to edit existing diary settings.
  - AddRemove - Ability to add or remove diaries.

- **rsmEditGrd** - Whether the user is able to edit grades.
  - None - No ability to edit grades.
  - Edit - Ability to edit existing grades.
  - AddRemove - Ability to add or remove grades.

- **rsmGroup** - Whether the user is able to edit security groups.
  - None - No ability to edit security groups.
  - Edit - Ability to edit existing security groups.

- AddRemove - Ability to add or remove security groups.

- **rsmRole** - Whether the user is able to create new or edit existing security roles.
  - None - No ability to edit security roles.
  - Edit - Ability to edit existing security roles.
  - AddRemove - Ability to add or remove security roles.

- **rsmScript** - Whether the user is able run scripts.
  - No
  - Yes

- **rsmTableDefaults** - Whether the user is able to edit the settings for tables.
  - No
  - Yes

- **rsmUser** - Whether the user is able to create new or edit existing users.
  - None - No ability to edit users.
  - Edit - Ability to edit existing users.
  - AddRemove - Ability to add or remove users.
  - AssignAdminGroups - Highest level of access, including ability to delegate the use of Retain Security using the 'Administrator for Groups' option against delegated users.

Retain Time

- **timeAdminLogon** - Whether the user is able to log on without an assigned resource.
  - N
  - Y

- **timeApproveJob** - Whether the user is able to approve by job (access Approve Job view).
  - N - No ability to approve by job.
  - View - Ability to view jobs and people allocated to each job.
  - Y - Ability to approve by job.

- **timeApprovePerson** - Whether the user is able to approve by staff (access Approve Person view).
  - N - No ability to approve by staff.
  - View - Ability to read timesheets against people.
  - Y - Ability to approve by staff.

- **timeApprover** - Whether the user is able to approve the timesheet.
  - N - The default value. No ability to approve the timesheet.
  - Y - Ability to approve the timesheet.

- **timeChargeView** - Whether the user can see the charge view.
  - N
  - Y

- **timeEditComponents** - Whether the user is able to edit the components.
  - N - The component view is hidden.

  - View - Ability to view components only.
  - Y - Ability to edit components.

- **timeEditJobs** - Whether the user is able to edit the jobs.
  - N - The jobs view is hidden.
  - View - Ability to view jobs only.
  - Y - Ability to edit jobs.

- **timeEditRates** - Whether the user is able to edit charge rates.
  - N - The rates view is hidden.
  - View - Ability to view rates only.
  - Y - Ability to edit rates.

- **timeEditResources** - Whether the user is able to edit resources.
  - N - The resource view is hidden.
  - View - Ability to view resources only.
  - Y - Ability to edit resources.

- **timeLimitJobs** - Whether the user is able to access the jobs according to the settings.
  - N - Ability to access all the jobs.
  - Y - Restricts access to jobs according to the settings.

- **timePeriodSetup** - Whether the user is able to edit periods.
  - N - The periods view is hidden.
  - View - Ability to view periods only.
  - Y - Ability to edit periods.

- **timeRetainTimeSettings** - Whether the user is able to customise settings.
  - N - No access to settings.
  - Y - Ability to edit the settings.

- **timeTimesheetEntry** - Whether the user can see the time view.
  - N
  - Y

- **timeValueView** - Whether the user can see the value view.
  - N
  - Y

- **timeReportingLevel** - Whether the user is able to view or edit reports.
  - Full - Ability to view and edit reports.
  - Default - Ability to view all the reports.
  - Own - Ability to view user's own reports.
  - None - No access to reports.

- **timeCanImport** - Whether the user is able to import timesheet.
  - No
  - Yes

- **timeCanExport** - Whether the user is able to export timesheet.
  - No
  - Yes

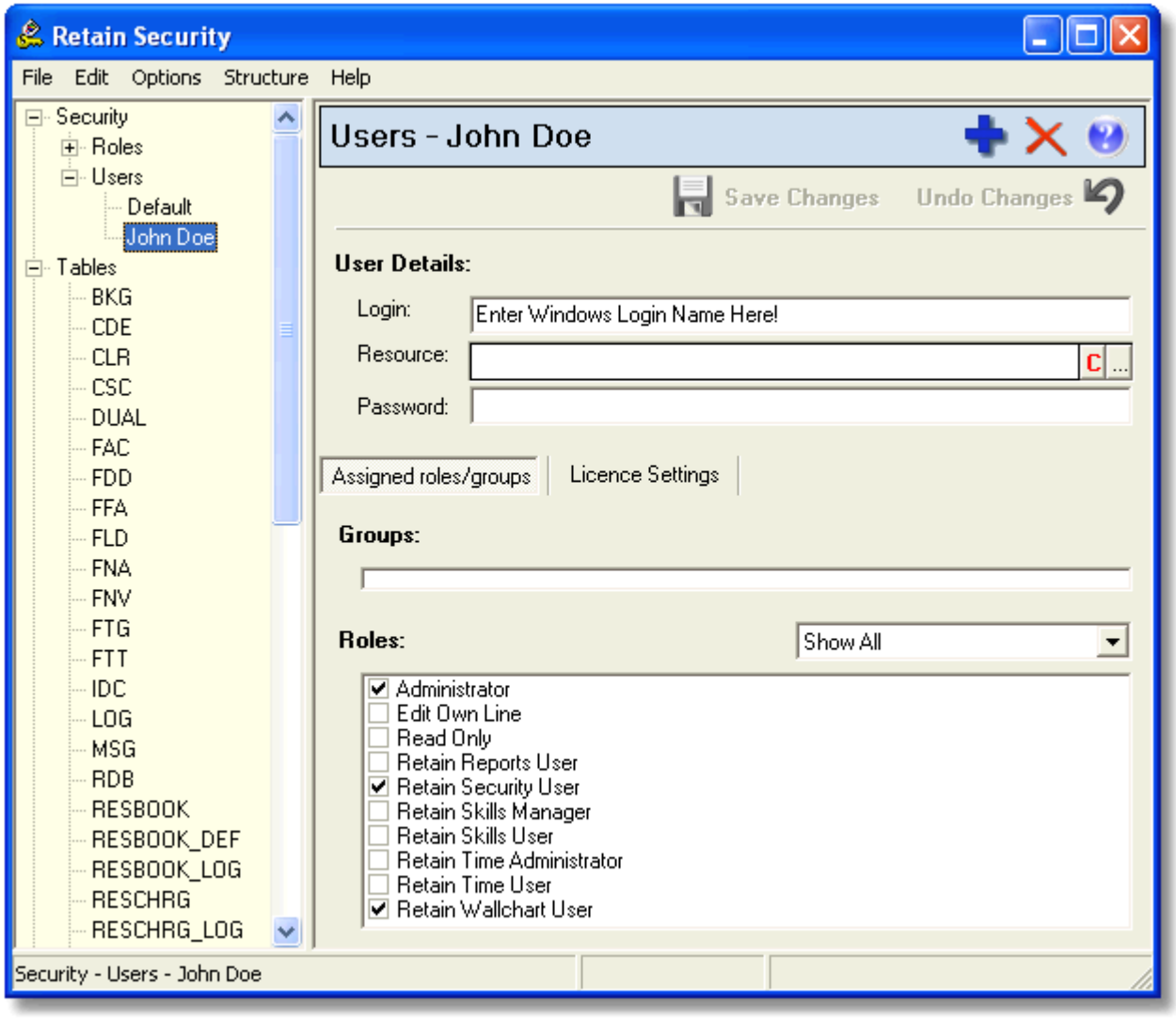
Miscellaneous

- **ChangeOwnPassword** - Whether the user is able to change his/her own password.
  - No
  - Yes

4.3 User Security

User security settings

When you open Retain Security for the first time it has an interface like the one below. This is where you create different type of roles and assign roles to a user.



Default user

Before any users have been set up in Retain Security there is only one user - 'Default'. We recommend that you never delete the Default user or modify the login details - you can change the roles assigned to it. A Default user initially has all the necessary roles so that anyone can access Retain and Retain Security. You require the Default user to have these roles to complete the initial setup. Once you have an Administrator user set up, you may want to change the roles assigned to the Default user to be a minimum set of roles.

Be careful not to remove the Retain Security access from the Default User until you are sure you have an alternative user with access to Retain Security.

The Default user is a special user:

- roles assigned to the 'Default' user are inherited by all other users.
- users who are not explicitly defined in Retain Security can log into Retain as the 'Default' user. For example, if you have many users who require read only access in Retain then instead of going through the time consuming process of adding each individual user, you can simply set the roles assigned to the Default user to the minimum and the read only users can log in as the Default user.

New user

To add a new user, for example an Administrator user:

- Right-click on 'Users' in the tree diagram in the left panel and select 'Add' or click on  button.
- Name this user e.g. Jane Doe.
- Login should be the same as the user's Windows login, which can be confirmed with the 'whoAmI.exe' utility.
- Resource can be selected if the user is also a resource in Retain and requires an 'Edit Own Line' role.
- Password should always be left blank unless you would like to password protect access to Retain.
- Save the changes by clicking on 

button.

You should not set up a password. Retain is set up to use the Windows user name to identify users and does not prompt for passwords by default.

Groups

A group is a collection of roles used in advanced implementations. You will see a list of groups that you set up earlier. You can assign a user group(s) by ticking the check box next to a group name. See Set up Groups for definition of groups.

Roles

The drop-down list on the right-hand side of the Roles section contains several levels of roles to select from, e.g. Functional or Row Level. See Set up Roles for definition of role types. You can use the drop-down to select the types of roles you would like to view.

'Show All' will display all roles:

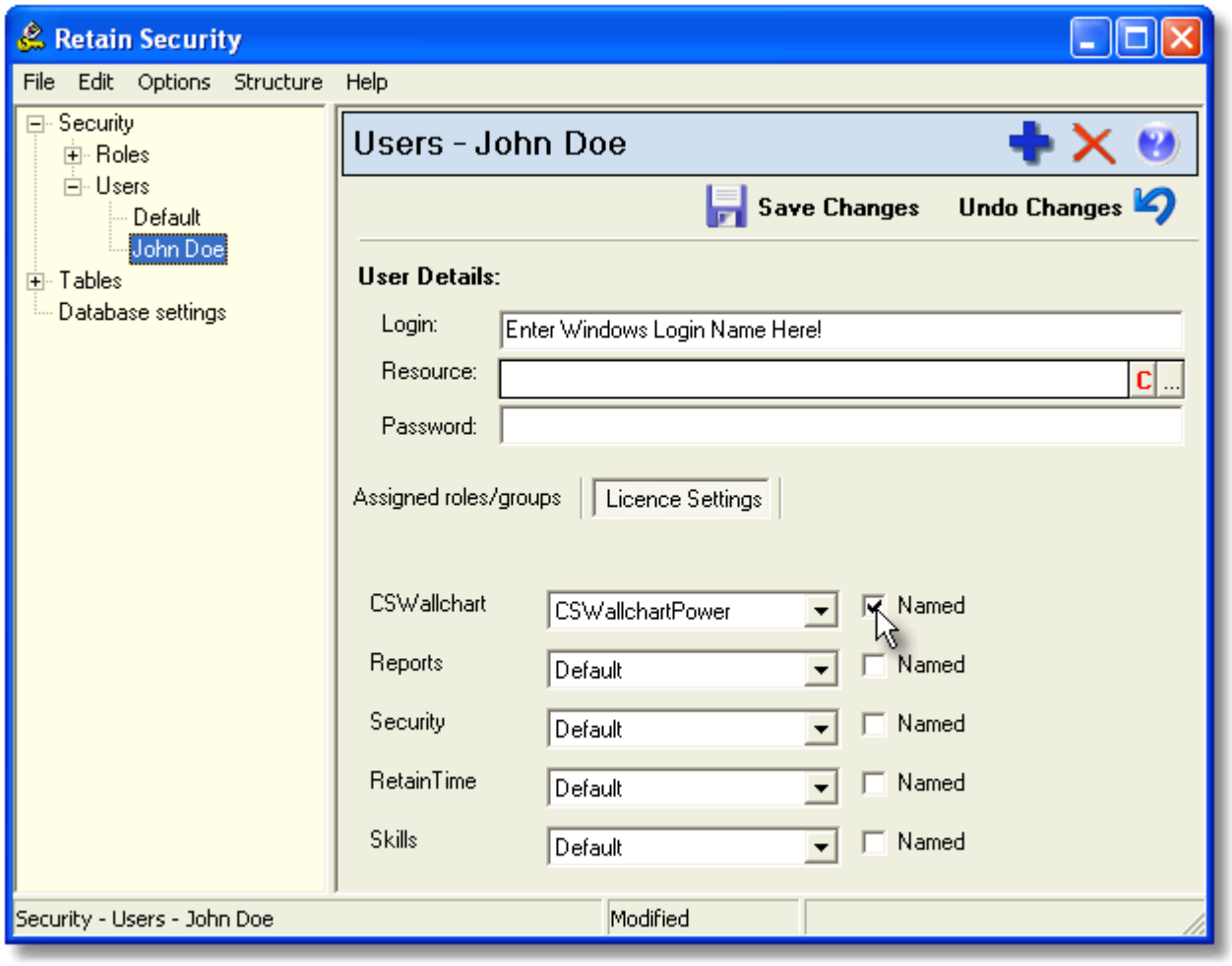
- Administrator - can edit data in Retain
- Edit Own Line - for a user who is also a resource in Retain
- Read Only - can view Retain but cannot edit
- Retain Security User - can use Retain Security
- Retain Reports User - can use Enterprise Reports module
- Retain Skills User - can user Retain Skills Query
- Retain Skills Manager - can user Retain Skills Manager
- Retain Time User - can use Retain Time module as a general user
- Retain Time Administrator - can use Retain Time module as an administrator
- Retain Wallchart User - can use Retain

Notes:

- Roles relating to Retain Skills, Enterprise Reports and Retain Time modules are used when the additional modules are installed.
- The Edit Own Line role allows a user to view the wallchart and add or edit bookings relating only to themselves. Be careful when assigning this role to the Default user.

Licence settings

Below the User Details section there is a Licence Settings tab next to Assigned roles/groups. Licence Settings allow you to further refine a user's levels of access to the Retain applications according to your licensing information. These should normally be left unchanged as Default.



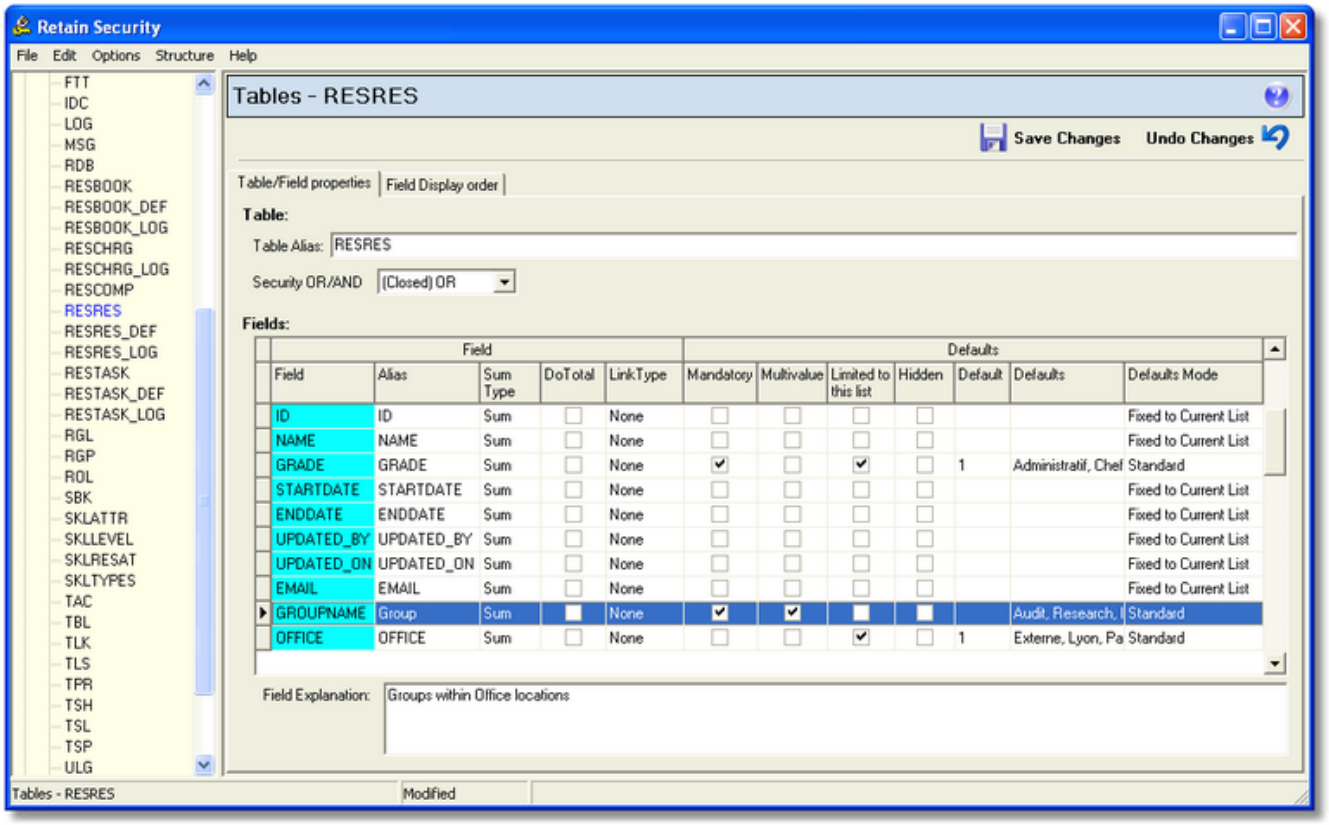
However, if you have named (fixed) user licence(s) instead of concurrent user licence(s), then you must select an access level from the drop-down list against the appropriate module and check the NAMED box.

5 Tables

5.1 Database table alias and default options

When viewing resource/job records or producing reports within Retain or Enterprise Reports module, users may want to see more descriptive field names as opposed to the generic field names in the database. Through the Tables option in Retain Security, you can define alias names for the fields used in Retain.

You can also define the behaviour of fields in the database when records are being added and edited.



To set up a table alias and define it's default options, select the table on which you wish to work by clicking on the table name in the left pane. The right pane will display the table.

- *Table Alias* – normally the default table aliases will be suitable. If they are not, you can edit the descriptive name for the table.
- *Security OR/AND* – OR option allows the fields used to define a field or row level access role to have 'either' relationship. (Open) OR is suggested to be used. AND option forces all field settings for a role to be satisfied when the role is used. See AND, OR (Closed) and OR (Open) Security.
- *Field* – this is the database field name, and cannot be changed.
- *Alias* – the alias can be edited to reflect the name users would prefer to see associated with the database field. This will be used in resource/job records and in reports as the column heading. Note that as a column header, you will not want it to be too long.
- *Sum Type* – you can change the default type to count, sum, average, show minimum or maximum. (For Enterprise Reports)
- *Do Total* – calculate total of all values in the field. (For Enterprise Reports)
- *Link Type* – this allows you to define a field as being used for path to a file. Only the File option is currently supported by Wallchart. Note that this does not store the actual file within the database, just the path to the file. Typically any paths should point to a common path on a file server.
- *Mandatory* – tick this box if this field must be completed (users will receive an error message and will not be able to create or edit the record unless there is an entry in this field).
- *Multivalue* – you can add more than one value to the field. For example, ticking the 'multivalue' box for the

'languages' field, you will have a drop-down menu within Retain where you can choose the necessary languages. (For Retain Enterprise)

- *Limited to this list* – tick this box if the only values allowed in this field are listed in 'Defaults'. Users cannot enter new values. They must select one from the list defined in 'Defaults'.
- *Hidden* – tick this box if you want the field to be hidden.
- *Default* – type here the value, if any, you would like to be pre-entered in the field when creating a new record.
- *Defaults* – define a list of values for users to select from when adding or editing records. Set the 'Defaults Mode' to **Standard**.

To add an entry, click the drop-down arrow to the right of the field (if there is no drop-down arrow, one will appear when you click in the field). Then click on the + button in the top right of the drop-down box. This will blank out the line and allow you to type in the data entry field at the bottom of the drop-down box.

To remove an entry, click on it to select it, then click on the - button in the top right of the drop-down box. To finish, either add another line to the list by clicking again on the +, or click elsewhere. Your selections will then appear in the Defaults field.

If you want Retain to use the values already in the database for the defaults for a particular field, type **__auto** (two underscores auto) in the Defaults box.

- *Defaults Mode* - set a mode for how defaults appear in Retain. Use defaults mode to control what data is entered into fields.
    - **blank -** same as 'Standard' mode.
    - **Standard** - users can enter any value into the field. If a list of values is predefined in the 'Defaults' box then users can select from this list.
    - **Fixed To Current List** - a deprecated mode. It can still be used to set fields as a free text field.
    - **Automaintained** - similar to 'Standard' mode but should only be used for booking fields e.g. RESBOOK.TEXT1. Generates a unique list of values from those already entered into the field.
- *Field Explanation* – field descriptions can help users add the right data into the right field when creating or editing records. This is shown in the status bar of the 'Add' and 'Edit' record dialog within Retain.

Notes:

- To avoid typing errors and synonyms, and to conform data to a standard, use *__auto*, but be sure to use it sparingly as it has an impact on the performance not only for individuals, but also for the whole system.
- Never use *__auto* in the Bookings table (RESBOOK or BKG) as it will severely impact performance (it will generate a list of unique values by searching the whole database each time a booking is made or changed). It is better not to use *__auto* for date and note type fields.
- For a well defined list, pre-define the values under Defaults column.
- If your entries in the field name or table name aliases do not appear to take effect after stopping and restarting the server then check that they are not being overridden by entries in the 'clntcfg.ini' file (see technical implementation guide).

Please note that changes are not applied until 'Structure | Effect changes' is selected from the menu in Retain Security or the server is stopped and re-started.

5.2 AND, OR (Closed) and OR (Open) Security

A user can be linked to multiple row level access roles. The Retain Security model offers three different ways of combining row level access for each table in the repository.

- **Open OR** is the most common way of thinking about the combination of rules. Given a record, all the rights granted from the different rules are added together. For instance, if one row level role is based on the OFFICE field and grants you *insert* and *update* rights, while another is based on the GROUP field and grants you *read* access; the complete set of access rights *(read, insert, update)* will be available to the user after assigning the roles.

- **Closed OR** is the default value and is similar to the **Open OR** security. The main difference is that when updating an existing record, if a field in one of the row level roles was not granting *edit* rights, that field cannot be changed to another value; whereas other fields in the record can be changed.

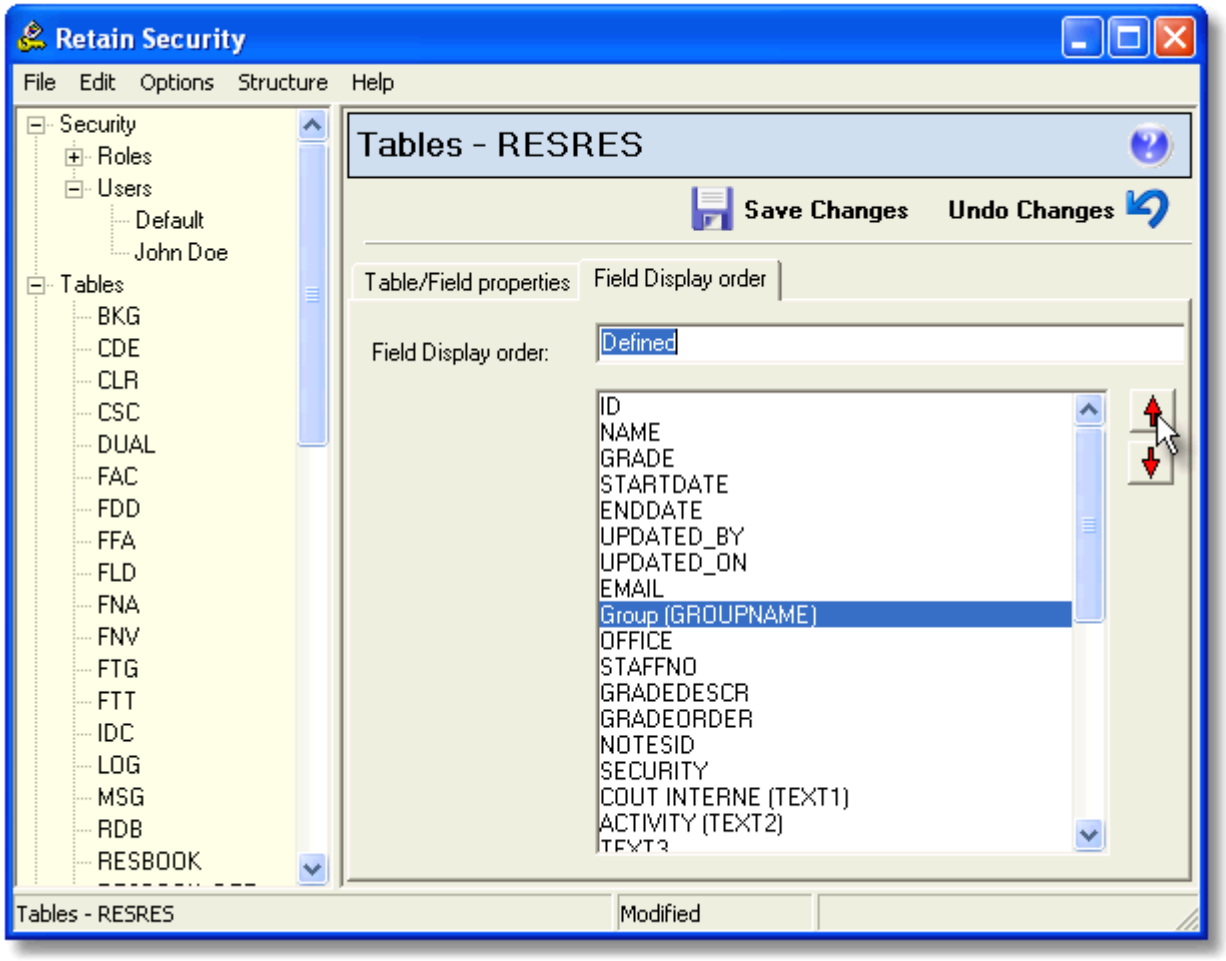
- **AND** is the most infrequently used condition. The set of rights granted on a record is the intersection of the sets of rights granted by a single role. If, for example, any of the row level roles grants no rights on a specific record while another role grants all possible rights; the user who has both profiles associated to it will have no access to the record. If one record has *read* access and another one *read* and *insert*, the resulting rights on that record would be *read* only.

To define AND/OR security for a given table, go to **Tables** section of Retain Security and select the required table. The AND/OR conditions can be defined using the drop down menu in the Table/Field properties tab.

Note that you can have different AND/OR conditions for different tables.

5.3 Field display order

The order in which fields are displayed in Retain can be changed.



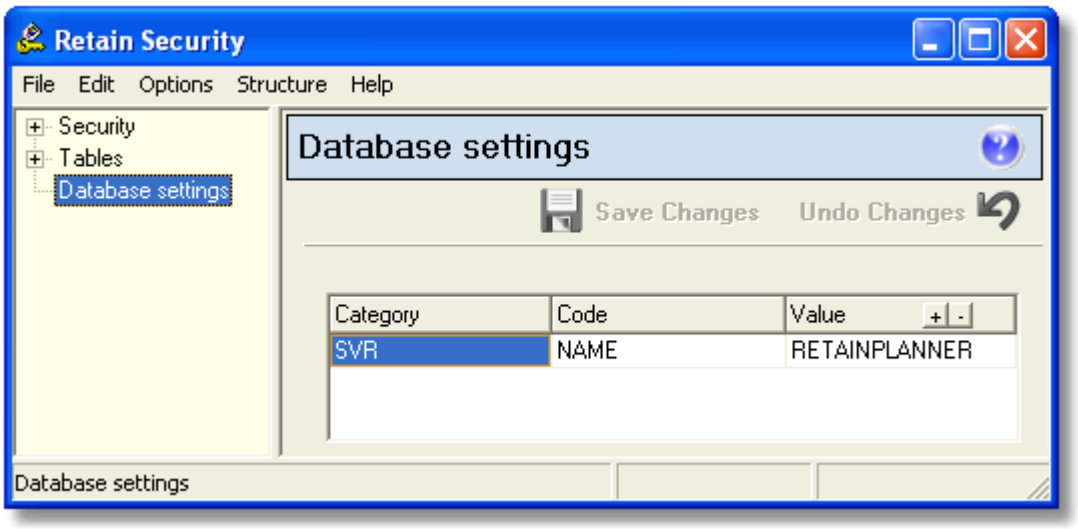
The Field Display Order can either be set to the "Default" from the drop-down list at the top of the form, where the forms within Retain will reflect the order within the database.

Alternatively, it can be set to "Defined" where you are presented with a list of all the fields, and the up and down arrow buttons on the left can be used to reorder the fields.

6 Database

6.1 Database settings

This is where you define properties against the database. You should not need to change the settings here unless you have more than one database server.

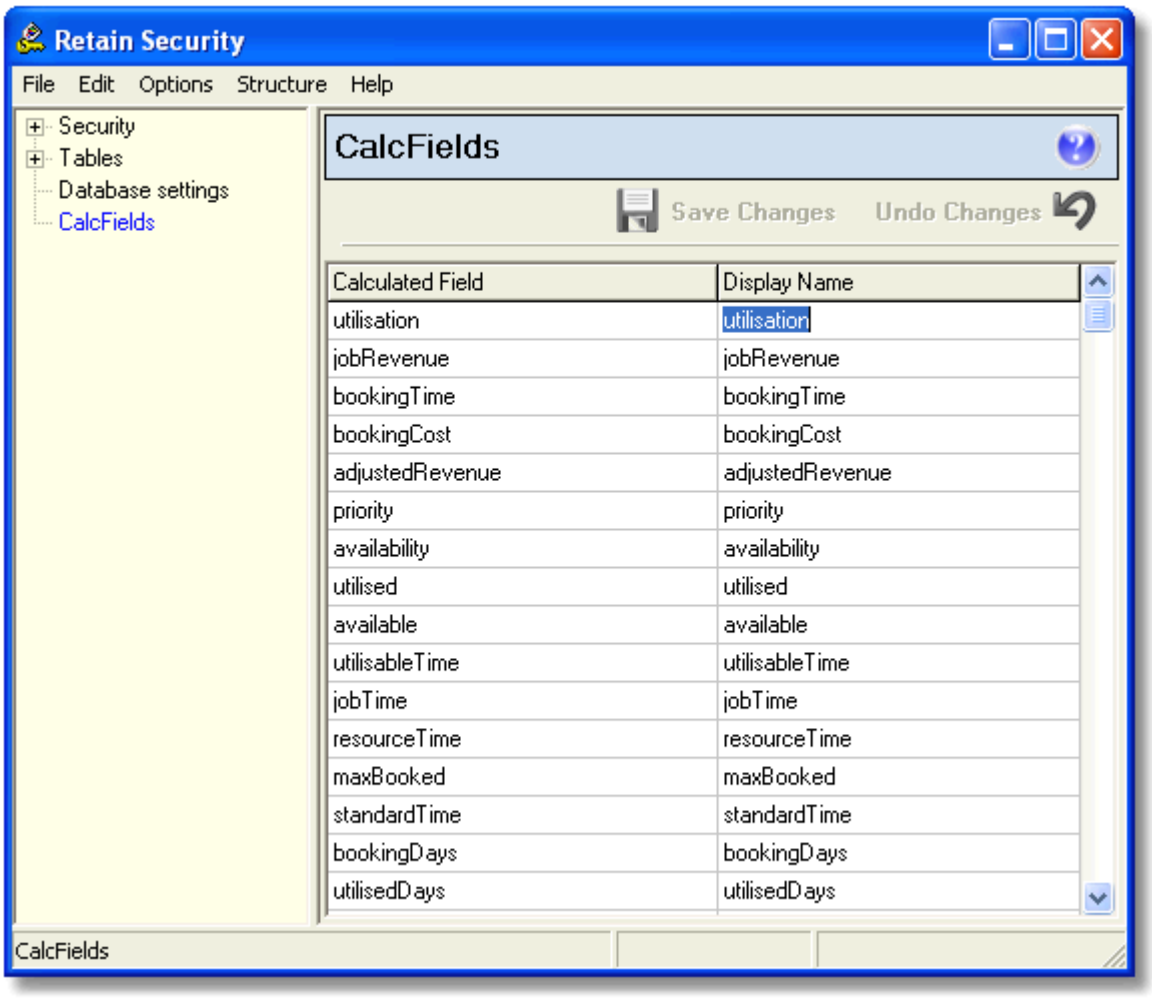


In the event there is more than one server, each one should have a unique name within the network. By default the server name is set to RETAINPLANNER or RETAINCLS, and this can be changed if necessary. The category and code columns should always be left unchanged.

7 Calculated Fields

7.1 Changing the description

Calculated fields are special fields used by Retain which return results based on a calculation. You can change the description (alias) of calculated fields for more meaningful descriptions in reports.



To rename a calculated field, select the Display Name and enter your description. Click on 

button to save changes after renaming

8 Appendix

8.1 Additional components

The components of the software available are:

Server

- Retain Server – server application that provides an interface to the database platform chosen.
- Retain Remote Server – manage several servers running across a network in a central location

Client

Core modules

- Retain – main resource planning application for viewing and manipulating resource and job allocations. It also has an internal reporting tool through which you can print wallcharts and calendars displayed on the screen, as well as writing and running simple reports.
- Retain Security – administration tool for defining user security, access rights, initial set-up of colour schemes, currencies, charge rates etc. and general management functions.

Optional modules

- Enterprise Reports – reporting module with full report designer and the capability both to design complex reports and to report across several databases.
- Retain Time - provides a time sheet system used for recording and managing time sheets.
- Retain Skills - captures and manages the skills within your organisation.
- Retain Importer - transfers or updates data from an external source into a Retain Enterprise database.
- Retain Notify – a companion module to booking requests for sending email notifications of changes in booking requests to resources and requesters.

9 Support

9.1 Support services

Support for Retain is available worldwide. This topic is linked to your support provider's information: Support Service Provider

retaininternational

USA:	1 877 819 8820 (toll free)
UK:	0845 458 8660
Australia:	+61 8 8346 2333
World:	+44 20 7538 4774
USA fax:	1 928 563 5137
Australia fax:	+61 8 8346 2133
World fax:	+44 (0)845 458 8661
E-mail:	info@retaininternational.com
Support:	support@retaininternational.com
Address:	33 Beaufort Court Admirals Way London E14 9XL United Kingdom

Index

- A -

access
  admin groups 11
  booking requests 11
  functional 11
  hints 9, 11
  reports 11
  rights 11
  roles 9
  security manager 11
  wallchart 11
access permissions 8
access rights 3
add a user 18
additional user 18
admin groups 9, 11
administration 3
Administrator 18
autopopulate role 9

- B -

Booking requests 3

- C -

calculated fields description 26
changes
  hints 21
client 3
conventions 4, 5
create a new role 8

- D -

data preparation 5
database
  alias 21
  defaults 21
  field names 21
  options 21
  preset values 21
  table 21
  value list 21
database servers listing 3
Default 18, 20
default role 8
default settings 20
default user 18
defaults
  automaintained mode 21
  database 21
  fixed to current list mode 21
  hints 9
  mode 21
  standard mode 21
  table 21
delete a user 18

- E -

Edit Own Line 18
exit 7

- F -

field properties 21, 26
fields 21, 26
  display order 23
  sort order 23
fields display order 23
functional access 5, 8

- G -

Getting started 6
Groups 5, 8, 18
  naming 5

- H -

Help 4, 28
hints
  access 9, 11
  auto 21
  changes 21
  database tables 21
  defaults 9

- I -

initial setup 3, 5
installation 4, 5
interface 7
Introduction 6

- L -

licence 20
Licence settings 20
licensing information 20
Login 6
Logon 6

- M -

main interface 7
maintain 3

- N -

naming 5
new features 4
new user 18

- O -

overview 6, 8

- P -

password 6
pick role 9
preparation 4, 5

- R -

Read Only 18
remove 8
rename 8
reports 3
resource planning 3
Retain Manager 3
Retain Reports User 18
Retain Security 18
Retain Time Administrator 18
Retain Time User 18
roles 5, 8, 18
  admin groups 9
  administration 9
  autopopulate 9

roles 5, 8, 18
default 9
edit own line 9
functional 11
logon 9
naming 5
pick 9
row 9
template 9
row level access 8

- S -

save 7
Security 6
Security Manager 3, 6
Security Manager overview 6
security model
and/or security 23
security options 5
server 3, 6
setup 4
Show All 18
starting security 6
structures 5
Support 4, 28

- T -

template role 9
thinking it through 5

- U -

user 5, 18
naming 5
user interface 7
user name 6
user security 3
user security overview 8
user security settings 18
user settings 18
users 8

- W -

Wallchart 3
who to use this guide 4

retaininternational
33 Beaufort Court
Admirals Way
London
E14 9XL
United Kingdom

646 688 4496 (USA)
0845 458 8660 (UK)
+44 20 7538 4774 (World)

info@retaininternational.com
www.retaininternational.com