HOW TO MANAGE USER SECURITY

This document describes how to create and edit users in Baseplan Enterprise, and how to create and maintain user security groups for Baseplan Enterprise users.

The Baseplan Enterprise security can be set on the following levels:

- Modules
- Screens
- Actions
- Views
- Menu Icons
- Buttons
- Functions
- Reports

Software Version: 1702

TABLE OF CONTENTS

PRE-REQUISITES

SQL Requirements

Administration users require:

- A domain user login to the Enterprise database
- User login to be a member of the 'SecurityBE' role
- User login needs to have the 'Alter Any Login' permission

Baseplan users who require access to GL Excel Add In and User Reports require:

- A domain user login to the Enterprise database
- User login to be a member of the 'QueryBE' role

Baseplan Enterprise Requirements

Administration users require:

- A user login to Baseplan Enterprise (as per Active Directory)
- Security Role 'Administrator'

All users require:

- An entry in the Active Directory, as the Baseplan Enterprise login credentials are based on the user's entry in the Active Directory
- A SQL login (non-domain account), as Baseplan users are replicated in SQL with a SQL login (non-domain account). When databases are moved from one server to another, you need to run 'ADD EXISTING USERS' from the Security – Users screen.

A domain username is different from the username created in Baseplan Enterprise. When a username is created in Baseplan Enterprise, the same login is automatically created in the SQL database. Usually, the domain user is manually created by a database administrator. A domain username has the following format: (Domain name\username).

USER SECURITY

1. From the Menu, select **Security > Users**

This will open the *Security – Users* screen.

The *Security – Users* screen is designed in 2 panels:

- Users
- Groups

Users are listed on the left side and Groups are listed on the right side of the *Security – Users* screen.

Right-clicking anywhere in the *Users* panel, displays a menu with the following functions:

- Add User
- Edit User
- Delete User
- Add Existing User

<u>Adding a User</u>

1. Right-click anywhere in the *Users* panel
2. Select **Add User** from the list of functions
3. Enter the relevant information
4. Click SAVE
5. Click CLOSE

This will close the *Users* screen and return to the *Security – Users* screen.

The added user will be listed under the *Users* panel on the left hand side of the screen.

Editing a User

1. Right-click on the user you wish to edit on the *Security – Users* screen
2. Select **Edit User** from the list of functions
3. Enter the relevant information
4. Click SAVE
5. Click CLOSE

This will close the *Users* screen and return to the *Security – Users* screen.

Removing a User

We recommend to set the user to 'INACTIVE' on the user record itself, rather than deleting the user.

Generally, inactive users are those who have left the company or have been transferred to different roles. These users no longer require access to Baseplan Enterprise.

Note: The **Delete User** option should be used in case of records that were created with an incorrect username, and have no transactions with their name.

1. Right-click on the user you wish to make inactive on the *Security – Users* screen
2. Select **Edit User** from the list of functions
3. Check the **Inactive** checkbox
4. Click SAVE
6. Click CLOSE

This will close the *Users* screen and return to the *Security – Users* screen.

An inactive user can be reinstated by clicking the SHOW INACTIVE USERS button on the *Security – Users* screen. This will add the user back to the *Users* panel. The record can then be edited to uncheck the **Inactive** checkbox.

Note: A list of all active users can be viewed by displaying the Permissions By User By Group – Summary report. The option **Exclude Resigned** must be selected to generate this report.

Groups

There are many predefined user security groups available within Baseplan Enterprise.

The predefined groups are listed in the right hand side of the *Security – Users* screen.

Assigning a User Security Group to a User

1. From the Menu, select **Security > Users**
2. Double-click on the user

This expands the already assigned user groups for this user (if there are any).

3. Click on the security group you wish to assign to the user
4. Drag and drop the security group onto the user
5. Release the mouse click
6. The security group(s) will be displayed under the user.

Removing a User Security Group from a User

1. From the Menu, select **Security > Users**
2. Double-click on the user

This expands the already assigned user groups for this user.

3. Click on the security group you wish to remove
4. Click REMOVE

This will remove the user group from the user.

CREATING A TEAM

This is for information purposes only.

1. From the Menu, select **Security > Configuration > Teams**
2. Add the required team
3. Click CLOSE

This will close the *Teams* screen.

USER/BRANCH RELATIONSHIP

The *User/Branch Relationships* screen provides the ability to grant access to specific actions for a branch that is not the user's default branch.

For example: A user has access to raise purchase orders through the relevant User Security group, which applies to the user's default branch only. If you wish to grant the user access to raise purchase orders for another branch, you would need to set the security access on the *User/Branch Relationships* screen.

1. From the Menu, select **Security > Configuration > User/Branch Relationship**
2. Add the required User/Branch Relationship
3. Click SAVE
4. Click CLOSE

This will close the *User/Branch Relationships* screen.

The table below lists the User/Branch relationships available in Baseplan Enterprise, alongside their respective functions:

USER/BRANCH RELATIONSHIP	FUNCTION
May Access Customer Collections	Allows the user to access collection records from other branches, in addition to their default branch, in the *Collection Notes History*, *Transactions* and *Rental Contracts* panels of the *Collection Details* screen. **Note:** The parameter **Implement User/Branch Relationship in Collections** must be enabled.
May Access Multiple Branches – Rental Contracts / Quotes	Allows the user to create and manage rental contracts/quotes for other branches, in addition to their default branch. **Note:** The parameter **Branch Security** must be enabled to use this function.
May Authorise Rate Changes	Branch parameters **Rental Rates – Lock Customer Rates Option** and **Rental Rates – Lock Non Customer Rates Option** determine if the rates that default on rental contracts can be edited. If rental rates are locked for editing, the **May Authorise Rate Changes** user/branch relationship can be assigned to the user for the relevant branch. When using this relationship to enable editing of customer-level rates, the **Customer Rates** checkbox on the *User/Branch Relationships* screen must be checked.
May Authorise Red Alerts	Red alerts are configured for cash customers. These alerts are displayed to notify the rental counter staff when a contract is created for the flagged cash customer. Red alerts are configured from **Rental > Configuration > Red Alert Types**. The *Alerts* panel in the *Cash Customer Details* screen is used to select the relevant notification. If a rental contract is created for a customer with red alert, the **May Authorise Red Alerts** user/branch relationship

USER/BRANCH RELATIONSHIP	FUNCTION
	can be used to allow the user to authorise the contract for the assigned branch, despite the alert.
May Authorise Stand Downs	If the value of the parameter **Authorisation – StandDowns** is '1' or '2', stand downs are required to be authorised. When enabled, the system checks if the user has authorisation to enter stand downs. User-level authorisation is configured from **Rental > Configuration > User Authorisation**. The **May Authorise Stand Downs** user/branch relationship allows the user to authorise stand downs for items on rental contracts created for other branches, in addition to their default branch.
May Authorise Sub Rental Orders	Sub rental supplier invoices with the **Auth. Required** checkbox checked must be authorised by a user with sufficient PO limits for Line Type 'S'. This user/branch relationship allows the user to authorise sub rental supplier invoices for other branches, in addition to their default branch. *Please refer to the 'How to Process Purchase Orders' and 'How to Process Sub Rental Contracts' for more information.*
May Override Damage Waiver	If the parameter **Do Not Allow Damage Waiver to be Changed on Rental Contracts** is enabled, the **Damage Waiver** checkbox on the *Equipment Rental* screen is locked. Assigning the **May Override Damage Waiver** user/branch relationship to the user for the required branch, allows the **Damage Waiver** checkbox on the *Equipment Rental* screen to be edited for the relevant branches.
May Raise Purchase Orders	Allows the user to raise purchase orders for other branches, in addition to their default branch. **Note:** To use this function, the **Use User/Branch Relationship when Raising Purchase Orders** parameter

USER/BRANCH RELATIONSHIP	FUNCTION
	must be enabled. Enabling this parameter will allow the user to select only the branches they have permission for, from the **Branch** field on the *Purchase Orders* screen. After the CONFIRM button is clicked on the *Purchase Orders* screen, the system will check the user/branch relationship for 'May Raise Purchase Orders' for the user in **Ordered By** field. If not found, the following message will be displayed: **Info:** "Cannot confirm this Purchase Order because you do not have the correct User/Branch relationship configured." If the parameter **Apply User/Branch Relationship for Minor Codes in Purchase Orders** is enabled and the parameter **Use User/Branch Relationship when Raising Purchase Orders** is also enabled, then the **Minor Code** drop down list on the purchase order detail line will be limited to the branches for which the user has a user/branch relationship.
May Receipt Purchase Orders	Allows the user to receipt purchase orders that were raised in branches other than their default branch. **Note:** To use this function, the parameter **Use User/Branch Relationship when Receipting Purchase Orders** must be enabled. If the parameter **Apply User/Branch Relationship for Minor Codes** in Purchase Receipts is enabled and the parameter **Use User/Branch Relationship when Receipting Purchase Orders** is also enabled, then the **Minor Code** for each receipt detail line will be checked against the user's user/branch relationship configuration. If any of the lines belong to branches for which the user does not have permission, then the RECEIPT GOODS and CONFIRM RECEIPT actions will be disabled in the *Purchase Order Receipts* screen.

USER/BRANCH RELATIONSHIP	FUNCTION
May Transfer from more than One Branch	Allows the user to process stock and equipment transfers from selected branches, in addition to their default branch.

MENUS

1. From the Menu, select **Security > Menus**

The available user groups are displayed in the *Groups* panel on the *Security – Users* screen.

Adding a New User Group

User groups make it easier to ensure all staff have the same permissions, and also to configure security permissions for new staff.

1. From the Menu, select **Security > Menus**
2. Click USER GROUPS
3. Click ADD NEW
4. Add the group details
5. Click SAVE

Note: Any changes made to the security access will be instantaneous.

For example: There are 3 user groups, 1 each for 'Accounts Payable', 'Accounts Receivable' and 'Rental Coordinators'. If you wish to grant user access to the General Ledger to the 'Accounts Payable' and 'Accounts Receivable' groups only, select the new group from the **Group** drop down list.

As a default, security access for the new group is disabled. You must check the **General Ledger** and **GL Menu** checkboxes.

The following message displays:

Info: "Are you sure you want to give access to the underlying menu items?"

If you select YES to the message, all the underlying menus and functions in the General Ledger will be checked and can be accessible for the User Security group. Go to the furthest level down and check/uncheck the required access for this User Security group. Where access has been granted, the security items are displayed with a suffix (W).

COPYRIGHT