User Authorisation using $AUTH32

1. Introduction & Overview

The User Authorisation system provided by $AUTH32 allows you to set up a table of authorised users with associated passwords and authorisation codes, who are allowed access, (or restricted access), to Global System Manager and applications containing Authorisation Point restrictions.

The system consists of three main parts:

- Authorisation Table maintenance;
- Global System Manager sign-on;
- Application level tasking.

The Authorisation Table maintenance utility ($AUTH32) allows the maintenance of the tables containing details of the users allowed access to both Global System Manager and restricted application.

The sign-on program ($AUTHEX) is used by Global System Manager to sign-on to restrict access to Global System Manager itself.

The application tasking is used to verify Authorisation Points within an application, and also to load any application Authorisation Points into the master authorisation tables.

2. Installations and Database Creation

In order to use this authorisation system you must create the $OPID database on unit $M. The DI$OPID file is a standard database dictionary which will be present on master SYSRES unit ($M). This must be used to create the $OPID database using the appropriate Speedbase utility. ($BADGN – Global database, $BADN – SQL databases, $BADC – C-ISAM databases).

Occasionally, a database upgrade may be required when upgrading System Manager. In this case appropriate instructions will be given on how to upgrade the database.

To activate this security system you must set the sign-on program to $AUTHEX by using the $CUS ‘customise sign on’ option. You will need to restart your system after doing this. **You MUST not set the authorisation program until you have added at least one user to the authorisation table using $AUTH32.**

3. Application Access Identification

To restrict access to an application the following identifiers are used:

- System-id
- Module-id

- Authorisation points

3.1 System-id

The system-id is defined by the System Administrator and can be used to differentiate between different versions or groups of application. An example may be an application being run for two different companies, COMPANY1 and COMPANY2, using the same program unit but different data units. The System Administrator may wish to set up COMPANY1 and COMPANY2 as two separate system-ids in order to define their access to the application separately. System-ids are specified on the menu line from which the application is being run, and this must be done using the Menu Maintenance utility, $MN32. A system-id is required for any application using Authorisation Points.

3.2 Module-id

The module-id is used by the application provider to identify a particular application. The list of module-ids for each product can be obtained from the software supplier.

3.3 Authorisation Points

An Authorisation Point identifier is defined by the software supplier and indicates points within the application where authorisation checking will take place.

The Authorisation Points for a particular system-id/module combination will not be loaded into the master authorisation file tables ($OPID on unit $M) until the application has been run at least once with an established system-id (i.e. one that has been entered using $AUTH32 and specified on the calling menu line). In addition, the Global System Manager authorisation program must be set to $AUTHEX for the Authorisation Points to be loaded. The System Administrator must run all relevant applications once the system-ids have been established before setting up application Authorisation Point vetting. In SP-24 and later it is possible to load the authorisation points from within $AUTH32.

In order to correctly establish access to application Authorisation Points it is important to be aware of the way access is checked.

For a particular Authorisation Point within an application the following initial checking is done in this order:

Access will be denied if:

- The system-id has not been set via the menu handler.
- The system-id/module combination has not been entered in the authorisation tables.
- The user is not present in the user tables and the system-id/module-id is controlled.

If the user is not present and the system/module combination is not controlled then access will be granted.

For users present in the user table the following checking now takes place:

Access will be granted if:

- The system/module combination override for that user has been set to not be controlled.

- The system/module combination override has not been set and the system/module combination is by default not controlled.

For users whose system/module combination override is set to controlled, or whose override is not set but the system/module combination is controlled, access is denied if:

- The user is not active.

- The user is not allowed access at this time.

- The Authorisation Point is not valid for this system/module combination.

- The access override for this system/module/Authorisation Point combination is for access not to be allowed.

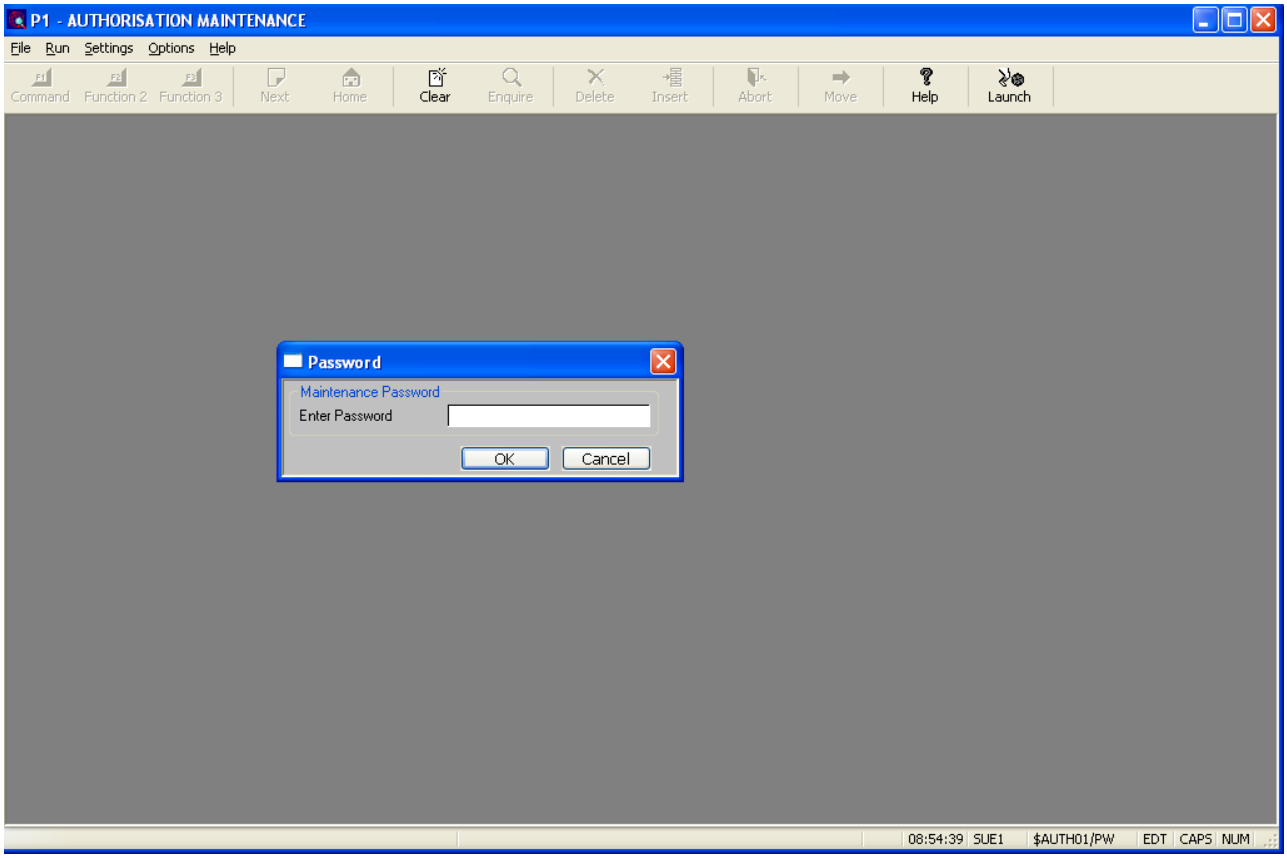
- There is no access override for this system/module/Authorisation Point combination, and the user is not a member of a group where the override access flag has been set to allow access, if the default access to this system/module/Authorisation Point combination is to deny access.

Now that access to this system/module/Authorisation Point is available, the user is asked to enter any password associated with the Authorisation Point. If the password has expired then the user will be denied access.

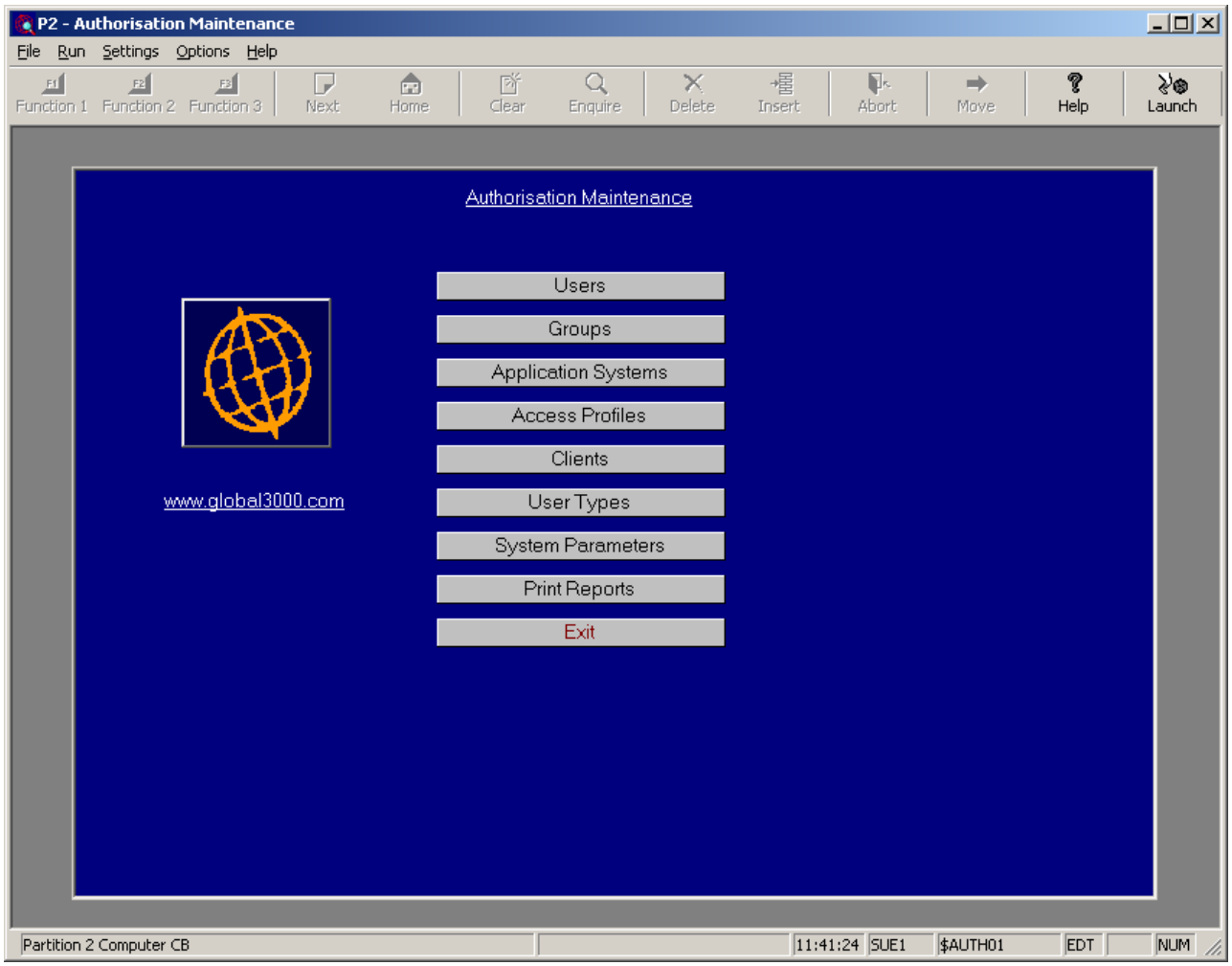
4. Authorisation Table Maintenance - $AUTH32

In order to run the $AUTH32 utility to update the authorisation tables database ($OPID in unit $M), a user must be established as a super user. The first operator to use the utility will automatically be entered as a super user.

On entry to $AUTH32 you will be asked to supply the maintenance password if there is one:

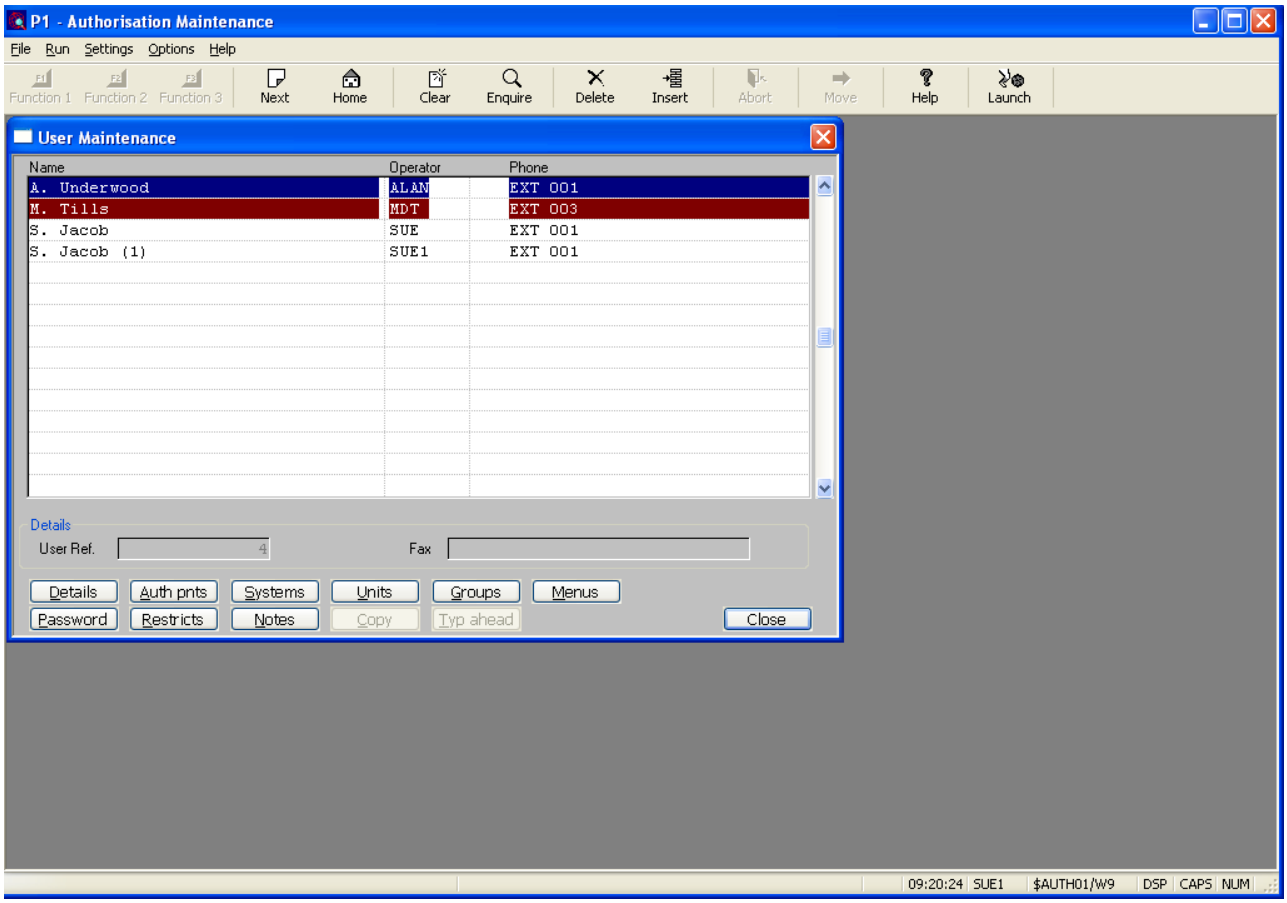


Having entered the maintenance password the following menu will be displayed. If there is no maintenance password $AUTH32 will start here.

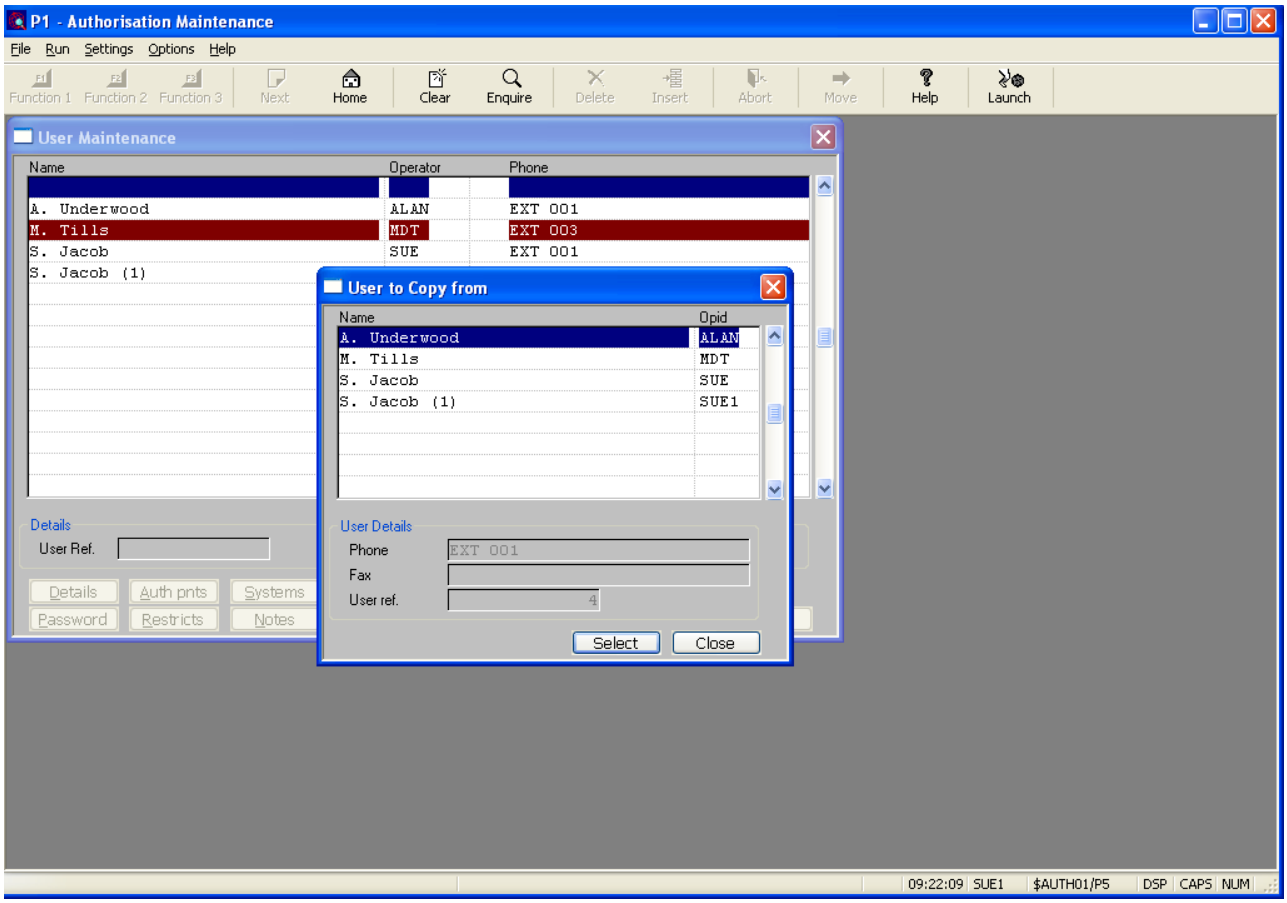


4.1 Users

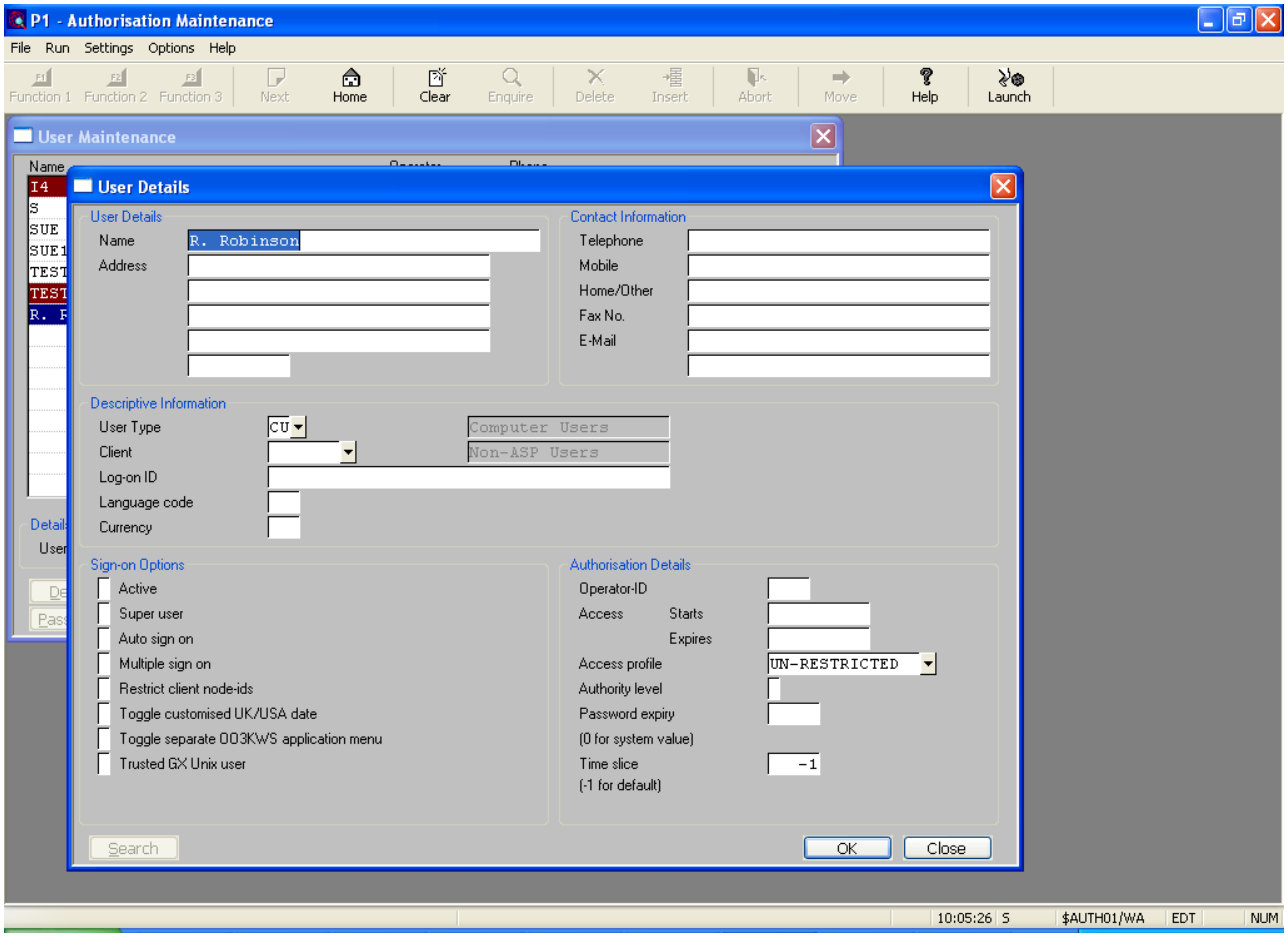
This function allows the definition of a table of users of the system. To add, modify or delete a user's details from the table of users you must select the 'users' option from the menu. The current list of users together with their operator-id and telephone number will be shown. Users who are in the table but are not currently active are indicated by a different colour.



To add or insert a new user, you should either position after the last entry or select the 'Insert' button from the toolbar. If you wish to copy the details of an existing user when adding or inserting, you should press the 'Copy' button. This will show you the table of existing users, allowing you to select a user to copy from.



When adding a new user, after entering the name, you will immediately be prompted for the user details:



4.4.1 User Details

4.1.1.1 Name, Address, Telephone etc.

You may enter the name, address, telephone numbers, Fax numbers and e-mail addresses for the user.

4.1.1.2 User type

You may select a type for the user. To display the list of available user types for selection, either presses the ‘Search’ button on the window, or key <UF1>. The user type CU (Computer user) is always available. To add further users types, select the ‘User Types’ entry from the menu. The user type is for descriptive purposes only. (see later)

4.1.1.3 Client

The client field may only be supplied if the application service provider flag is set in System Parameters. Clients may be added by selecting the ‘Clients’ option from the main menu. The client field is currently for specialised descriptive purposes only and will generally not be required. To view the current list of clients and to select one, either press the ‘Search’ button on the window, or key <UF1>.

4.1.1.4 Logon-id

The logon-id may not be entered and is available for future use.

4.1.1.5 Language code

You may set a language code for the user. This is for descriptive purposes only and has no connection with the language code used for GX translation.

4.1.1.6 Currency

You may set a currency for the user. This is for descriptive purposes only and has no relation to the currency used for Global 3000 applications.

4.1.1.7 Active

You may flag the user as active. A user who is not active is considered (for authorisation purposes) as if they are not in the user table.

4.1.1.8 Super user

You may set the user to be a super user. Only super users are allowed access to $AUTH32. You must have at least one super user in the user tables.

4.1.1.9 Auto sign on

The auto sign on flag is used to specify automatic or manual sign-on for the user. If the auto sign-on flag is set, then once the user has signed on once for a particular Global System Manager user number, they will be signed on automatically to that user number the next time Global System Manager is entered.

4.1.1.10 Multiple sign on

This flag is only effective if the ‘Allow multiple sign-on’ system customisation has been set to honour the ‘authorisation’ utility in $CUS. If the multiple sign-on flag is set, the user may sign-on to Global System Manager with the same operator-id more than once.

4.1.1.11 Restrict node-ids

This option allows you to restrict a user to a set of client node-ids. If this option is selected, you may key up to four client node-ids in the ‘Authorisations Details’ section of the window to which the user has access.

4.1.1.12 Toggle customised UK/USA date

This allows the USA date format flag to be set to the opposite value for this user to that set for the system using $CUS.

4.1.1.13 Toggle separate OO3KWS application menus

This option is available in GSM SP-23 and later and allows the separate OO3KWS application to be set to the opposite value for this user to that set for the system using $CUS. This flag is used to control whether application menus appear in the menu tree or as menus in the application tabs in a OneOffice3000 environment.

4.1.1.14 Trusted GX UNIX user

This is a specialised option only for use on Unix systems. Users marked as a trusted user and signing-in via GX will not be prompted for the System Manager password.

4.1.1.15 Operator-id

This is the four-character operator-id, which the user must use to sign-on to Global System Manager. All operator-ids must be unique. For GSM SP-23 and earlier the operator-ids must be upper case. For GSM SP-24 and later the operator-ids may be in lower case if the 'Allow lower case operator-ids' system parameter has been set (see later).

4.1.1.16 Access

You may specify a start date and expiry date over which this user is allowed access. If no date is set then there is no access date restriction.

4.1.1.17 Access Profile

Access profiles are a further way of restricting the access time of a user. An access profile of 'UN-RESTRICTED' is always available and allows unrestricted access. Further access profiles can be set up running the 'Access Profiles' entry from the main menu. To view and select the current access profiles press the 'Search' button on the window.

4.1.1.18 Authority Level

This is the Global System Manager authority level (A-Z) allocated to the user after signing on to Global System Manager (A being the lowest and Z the highest). Users with authority levels of S and above are considered by Global System Manager as supervisors and will be allowed access to certain utilities not available to users with lower authority.

4.1.1.19 Password expiry

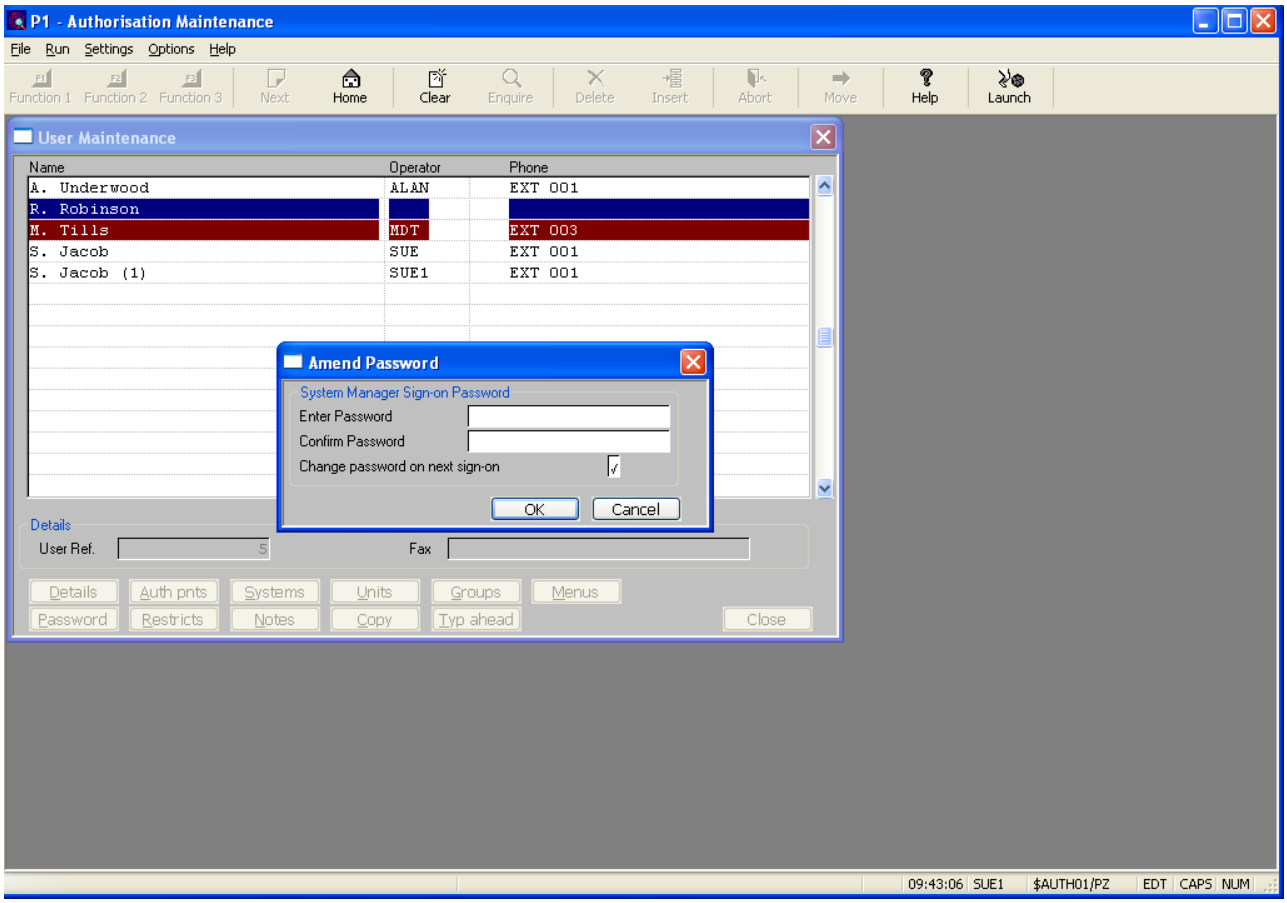
The password expiry period is the number of days for which the Global System Manager sign-on password is valid. If a user signs on after the password has expired a change of password will be forced. The user password expiry overrides the password expiry set in the 'System Parameters' entry from the main menu. A value of 0 to the user password expiry days will cause the password expiry to default to the password expiry for the system.

4.1.1.20 Time slice

This allows you to modify the times slice for a user. This is a specialist option and should normally be set to –1 to indicate that the default should be used.

4.1.2 Completing the User Details

Once you have entered the user details you will be forced to enter a Global System Manager password for the user.

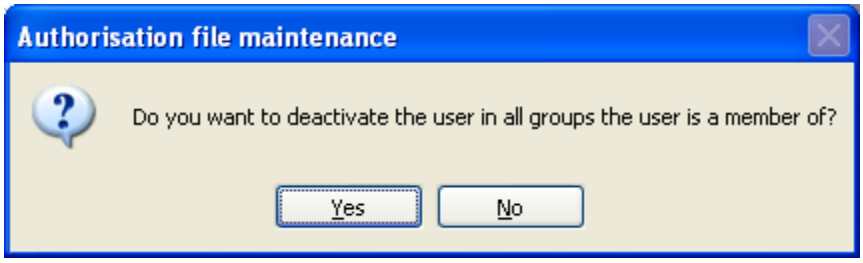


In general you would supply a starting password and set the flag to force the user to change the password on next sign-on to Global System Manager. For GSM SP-24 and later you may set a default password in the system parameters (see later). This password will be used as the default password in the password window avoiding the need to enter the starting password each time.

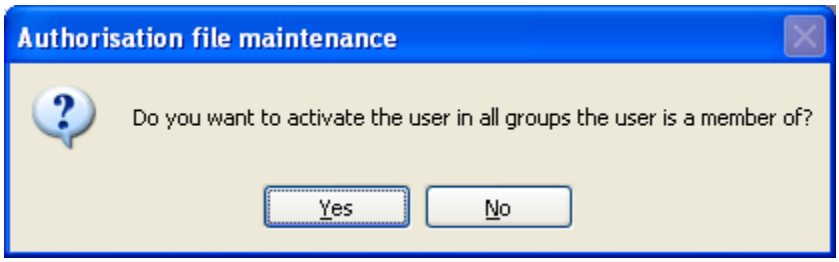
To delete an existing user from the list, you should position on that user and select the 'Delete' button from the toolbar. You will be asked to confirm deletion.

To update the details for a current user, you must position on that user and select the appropriate maintenance button

If an already existing user has the active status modified you will be asked id you want to change to active status for all groups the user is a member of.



or



Pressing the 'Yes' button to either question will set the active status of the user within groups the user is a member of to the relevant value.

4.1.3 Details

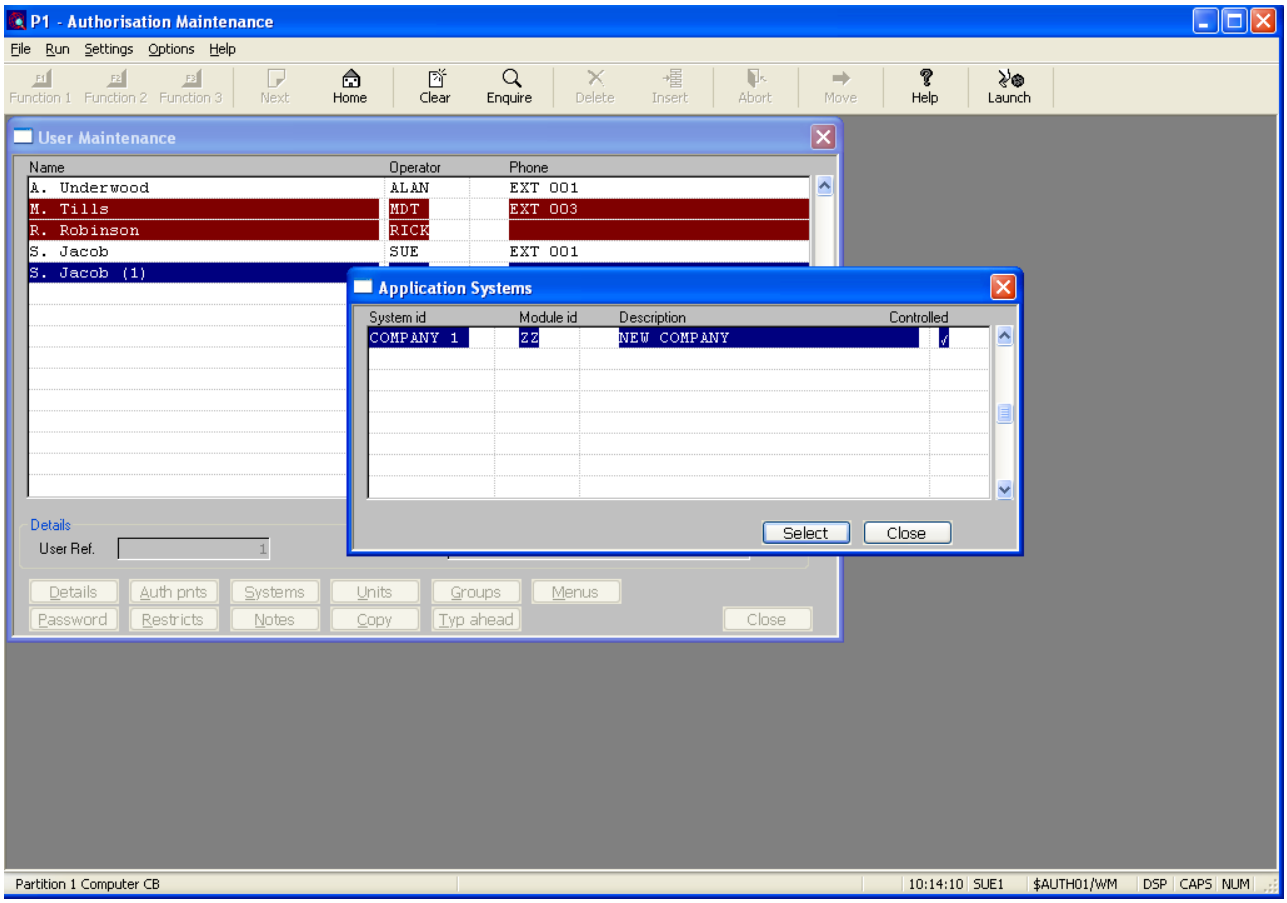
This allows you to amend the user details as above.

4.1.4 Password

The password button allows you to change the user's current Global System Manager sign-on password.

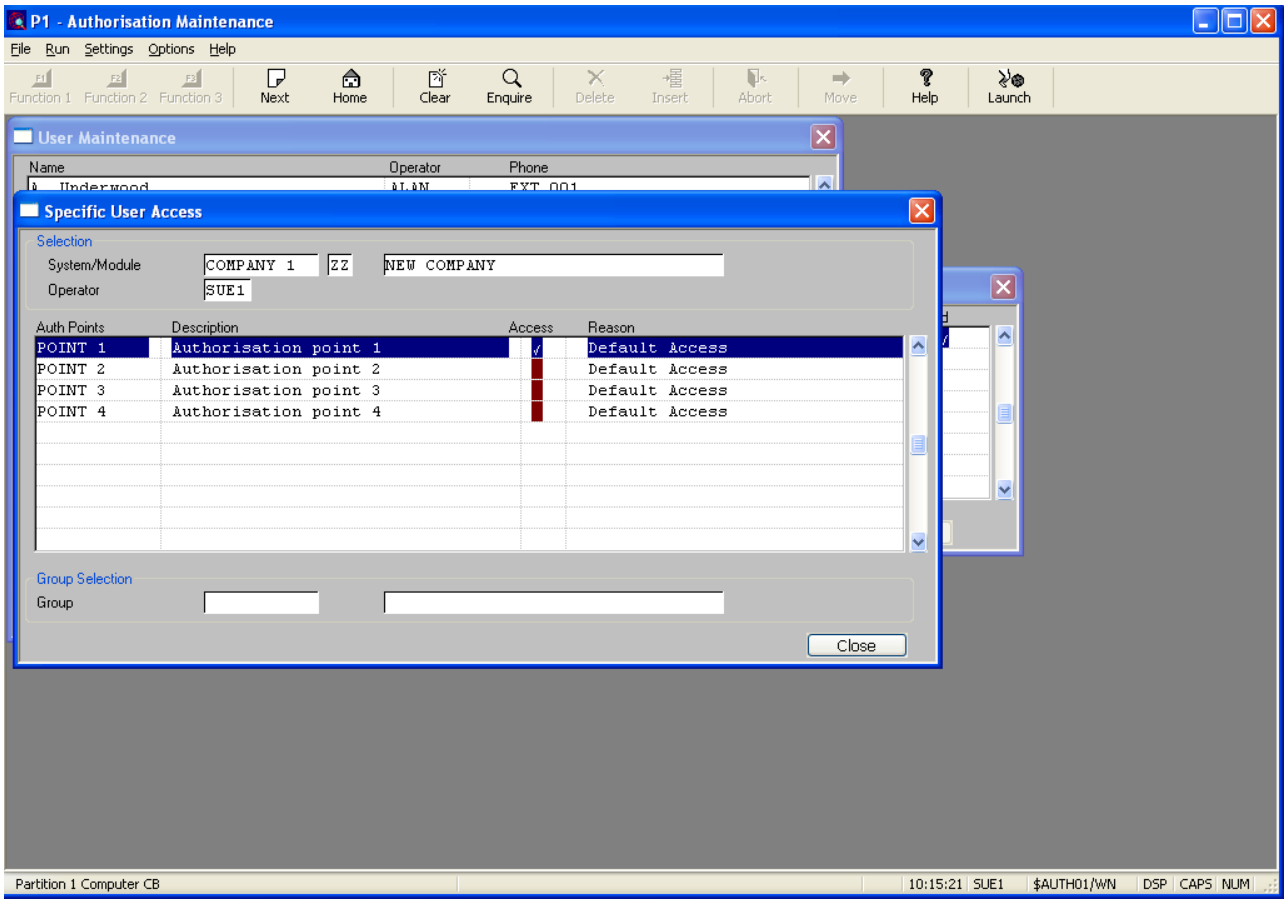
4.1.5 Auth Pnts

As described above, Authorisation Points are loaded into the authorisation tables when an application is run for the first time with a defined system/module combination. For GSM SP-23 and later it is possible to load the authorisation points from the 'Application systems' option from the main menu. The 'Auth pnts" button allows you to view the list of authorisation points available for the system/module combinations for which access is specified for the current user. The systems available to that user must previously have been set using the 'System' button from this window.



You must select the System/ Module combination that you wish to view.

The Authorisation Points will then be shown:



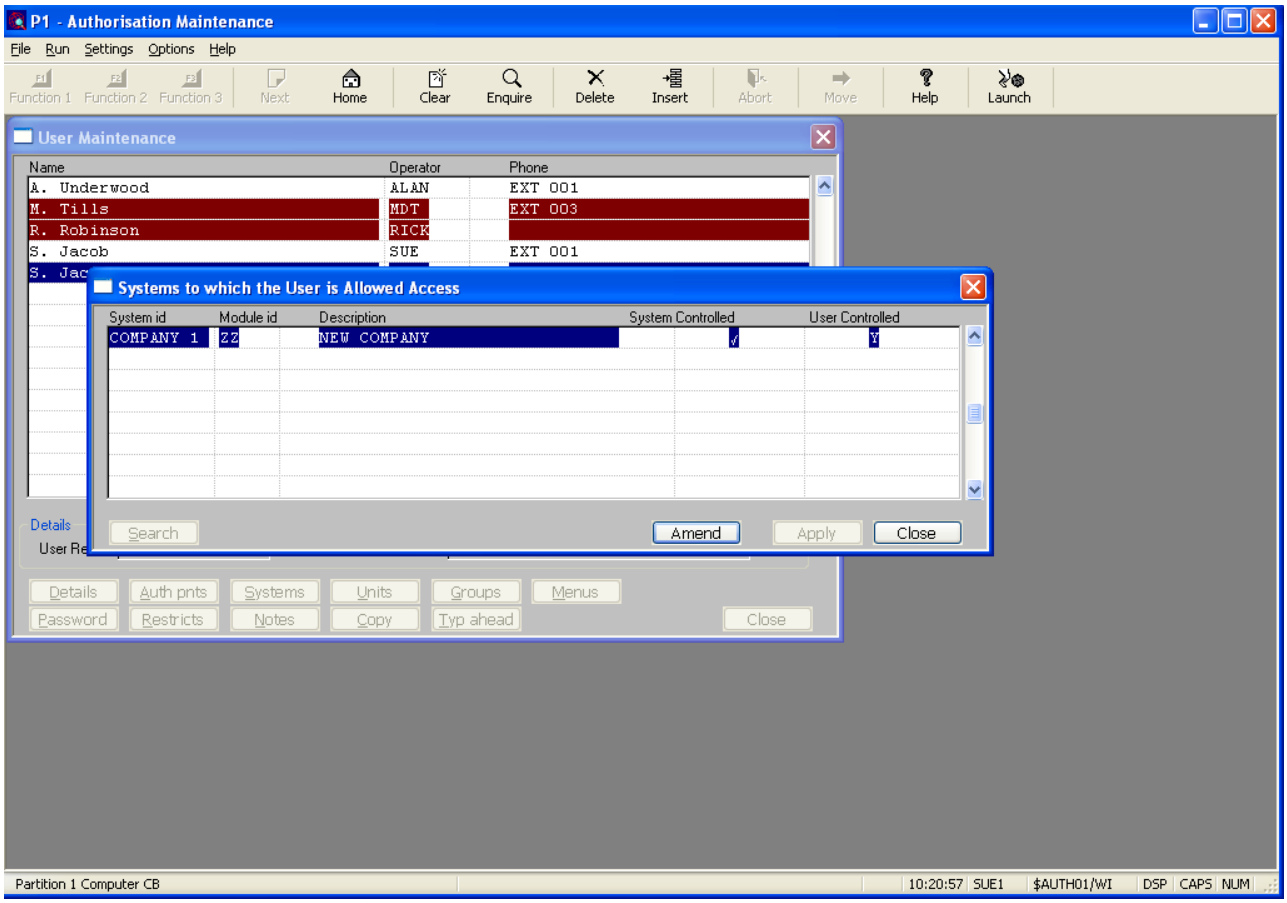
The coloured tick boxes just highlight authorisation points where access is denied.

4.1.6 Restricts

User restrictions should not be set as they are for future use.

4.1.7 Systems

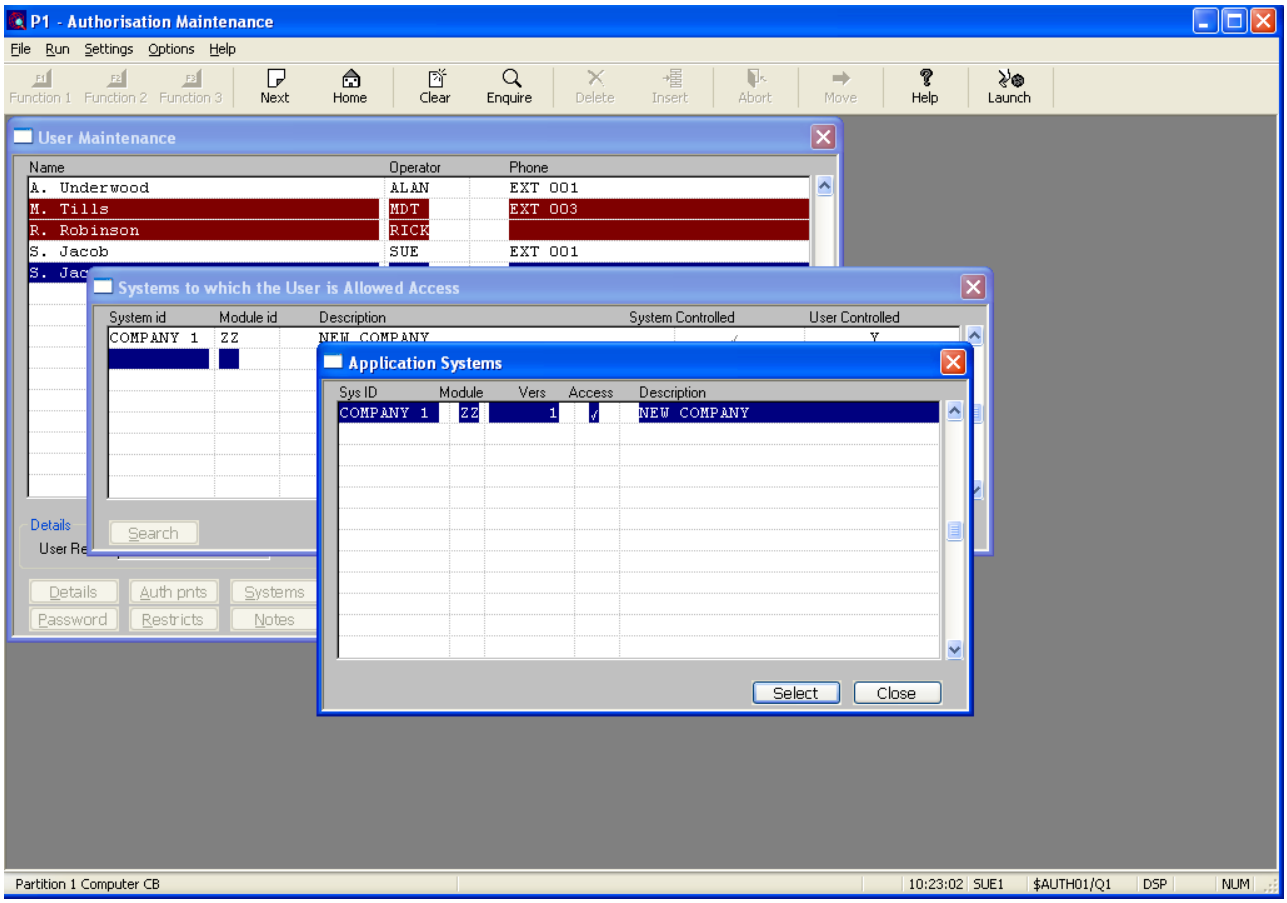
System/module combinations are defined by selecting the 'Application systems' option from the main menu. The 'Systems' button here allows you to add or remove systems associated with the user, for which the user's access will be defined.



You may amend the user-controlled flag for a system/module combination. Setting this to “Y”, means that you want access to this system/module combination to be controlled for this user. Setting it to “N” indicates that you do not want to control its use. Setting it to SPACES means that you want to default to the ‘default control’ flag for that system/module combination.

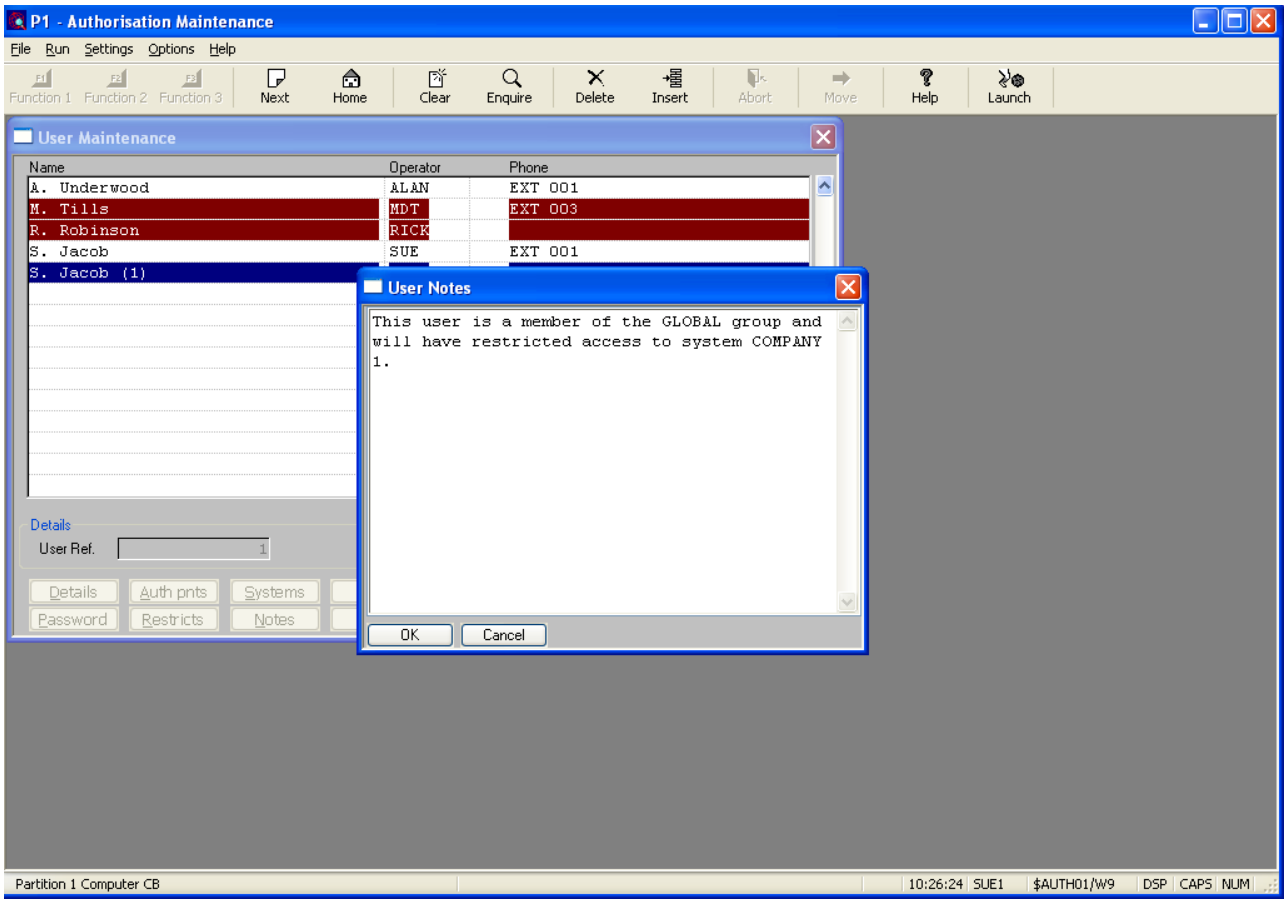
You may delete a system/module combination by selecting the ‘Delete’ button from the tool bar.

To view and select the system/module combinations available, press the ‘Search’ button in the window



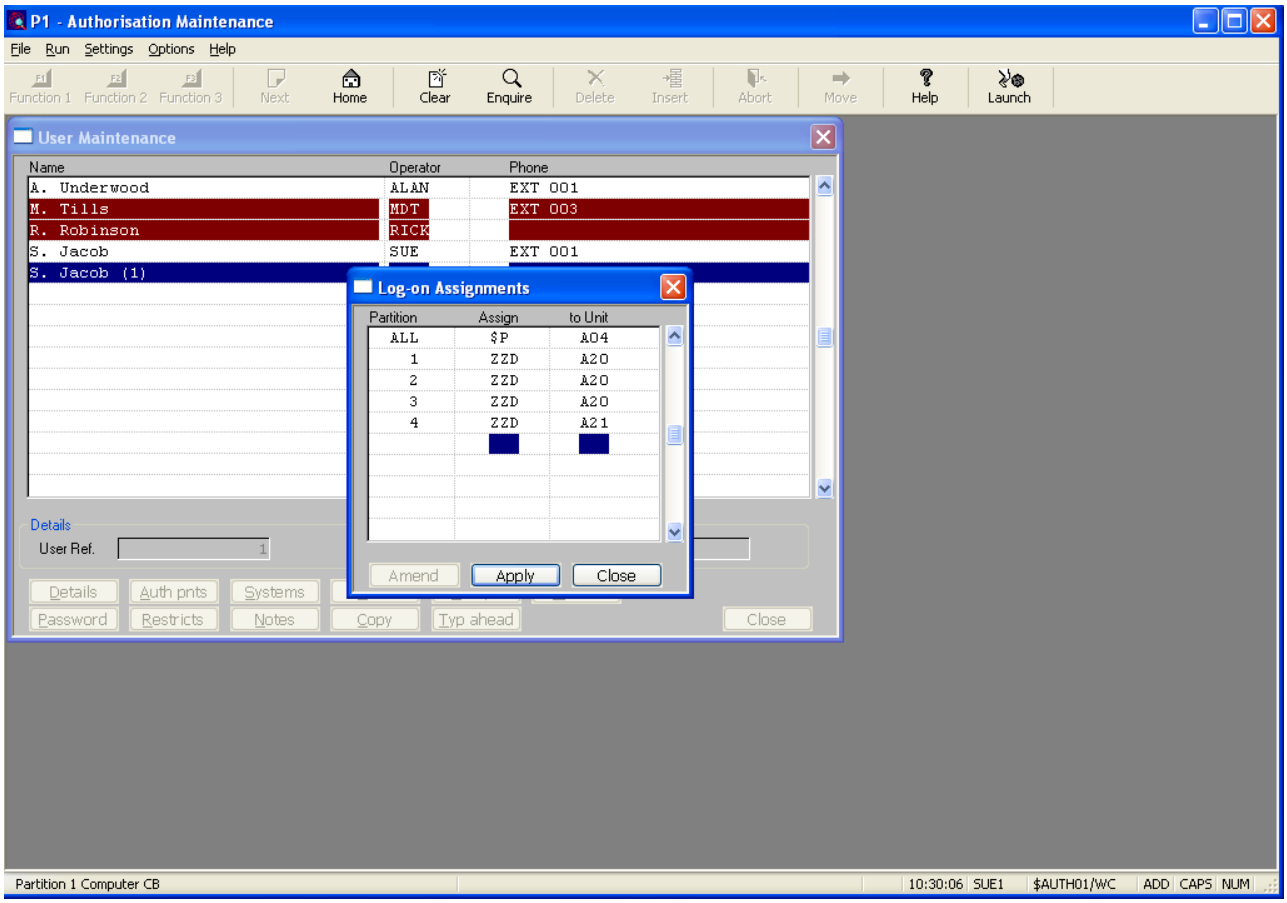
4.1.8 Notes

Pressing the notes button allows you to enter free format notes associated with the user.



4.1.9 Units

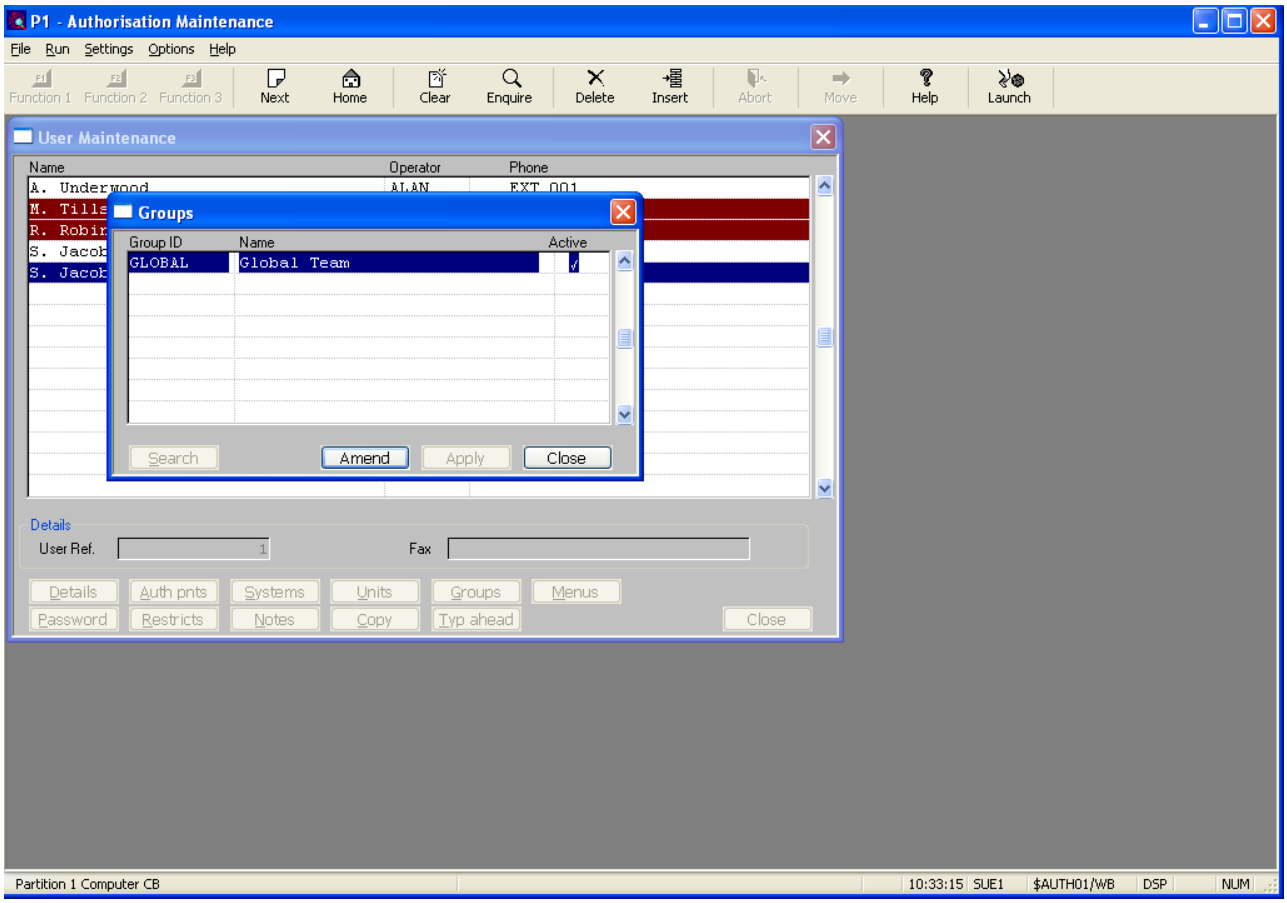
You may set unit assignments on a per-partition basis. Note that it is not advisable to set per-partition assignments in a OneOffice3000 environment.



These unit-ids will be assigned when the user signs-on to Global System Manager. If an assignment is required for all partitions 0 can be keyed to the partition number.

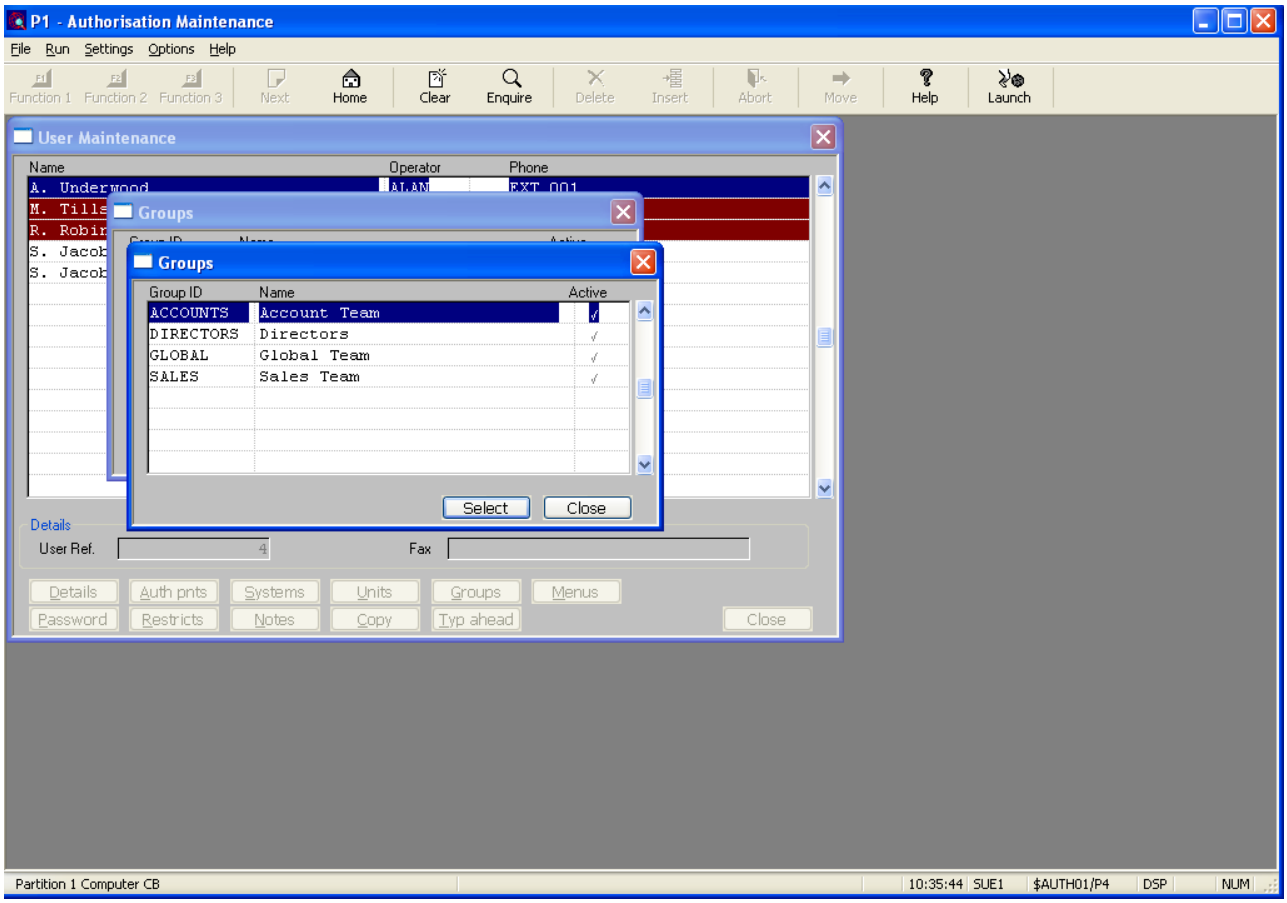
4.2 Groups

Groups are defined by selecting the ‘Group’ option from the main menu and are used to gather together a group of users. To select the groups to which the user should belong to press the ‘Group’ button.



You may delete groups from this list by selecting the ‘Delete’ button from the tool bar.

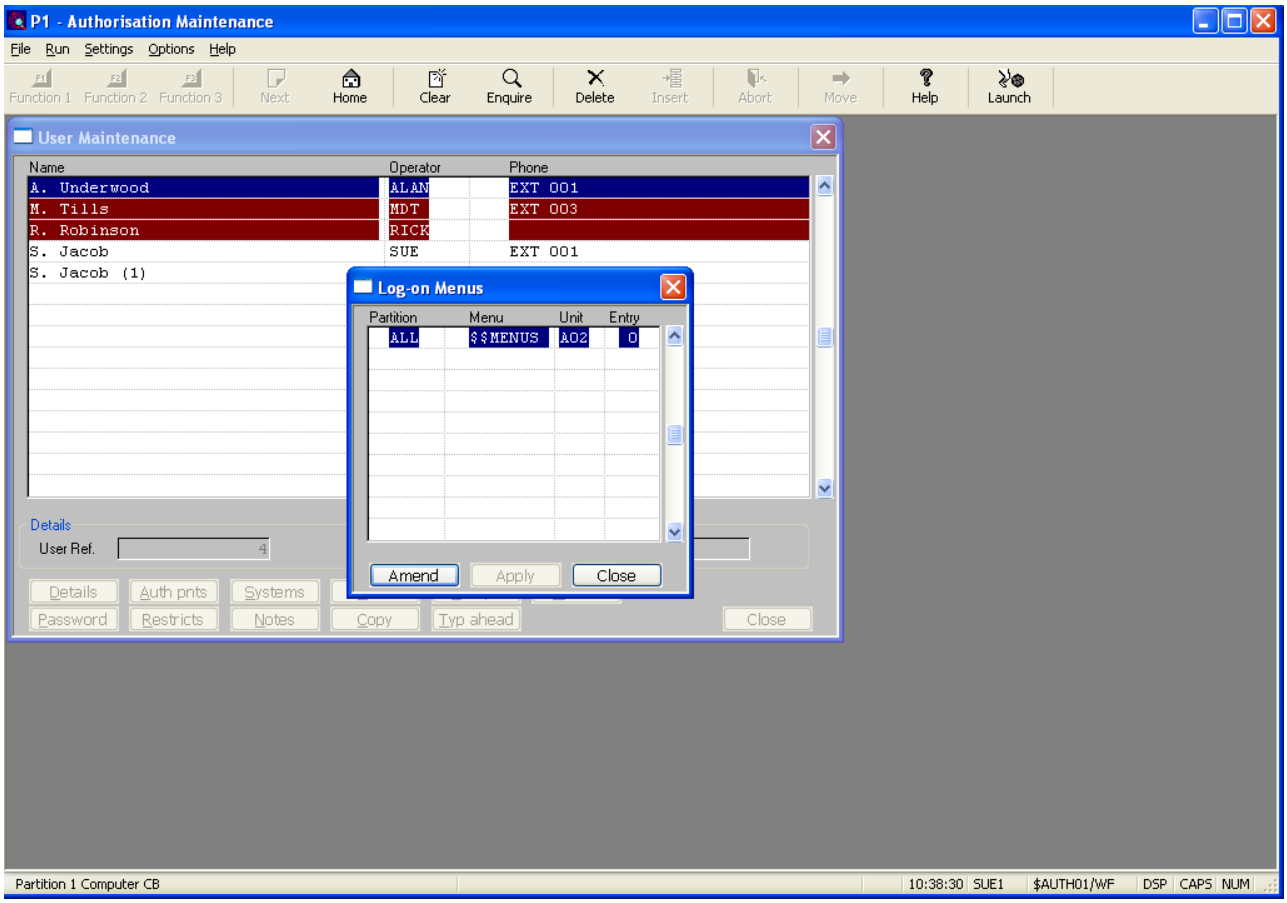
To check the list of existing groups and to select one, press the ‘Search’ button on the window



You may select an additional group for the current user.

Menus

You may set up an initial menu file and menu line for the partitions for the selected user:

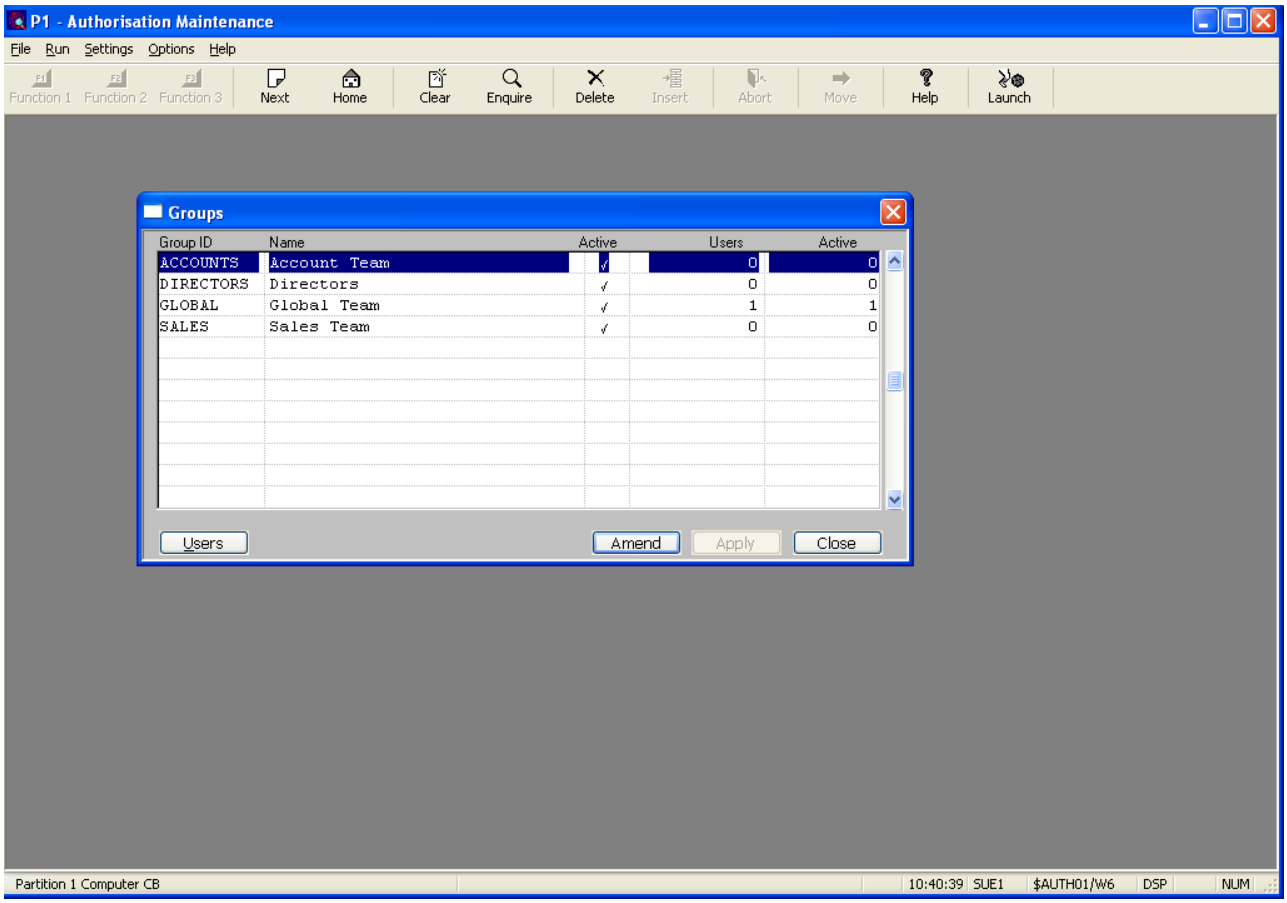


The menu file indicates the menu which will be entered when the user signs-on. If you do not specify a menu file then the menu file $$MENUS on $DP or $M will be entered on sign-on. If you want a menu line on the first menu page of the menu file to be executed on sign-on then you need to supply the line number in the 'Entry' column. A line number of 0 indicates that no menu line should be executed.

If you want the menu information to be applied to all partitions you can enter 0 to the partition number. Note that you must not set menus on a partition basis in a OneOffice3000 environment.

4.2 Groups

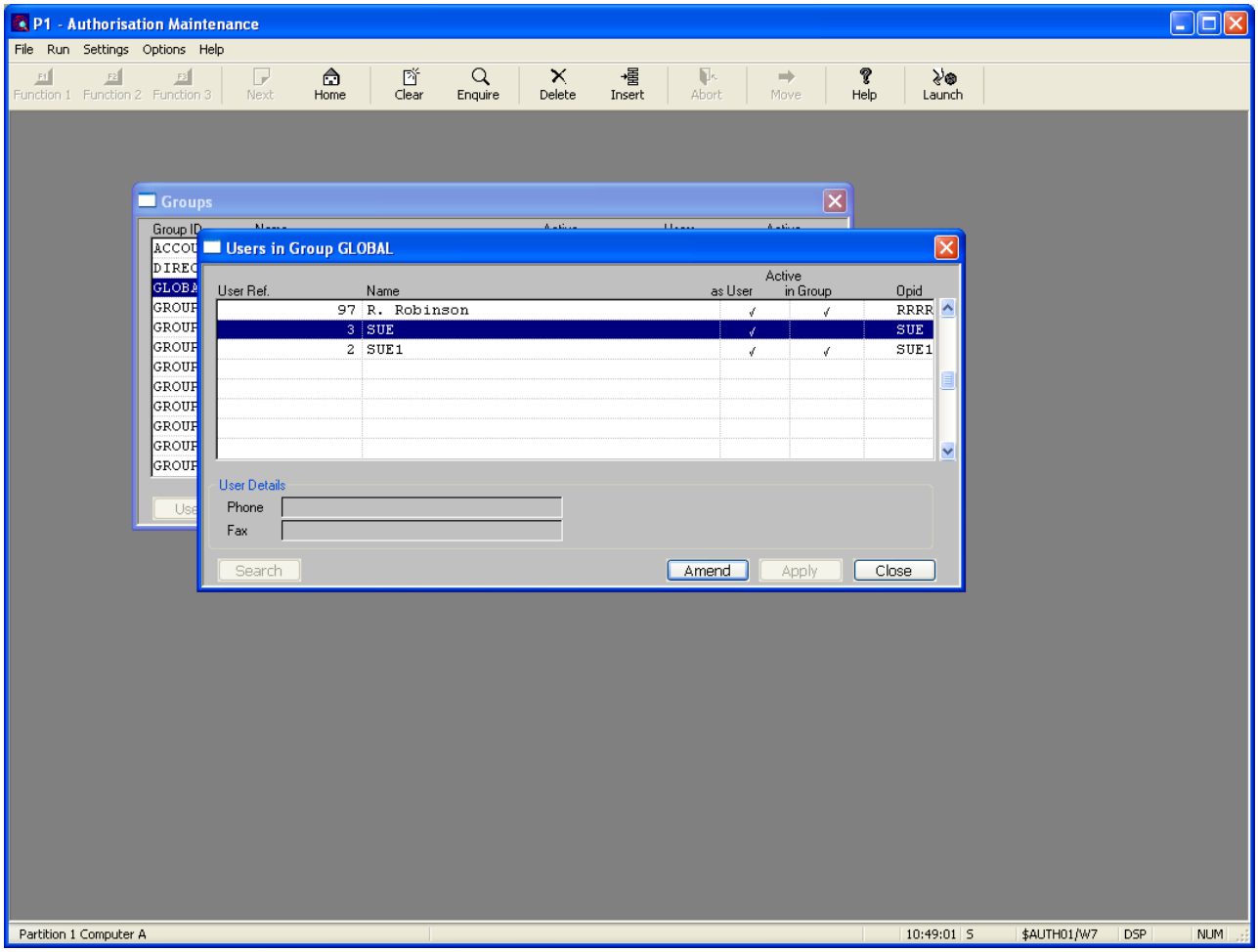
You may group together users and define their security access together as a group. To modify the group details you must select the 'Groups' option from the main menu.



To delete an existing group you must position on the group and press the ‘Delete’ button from the toolbar.

You may add an additional group to the end of the list by entering the group name and description.

To update the list of users who are members of a group, you must press the ‘Users’ button on the window.



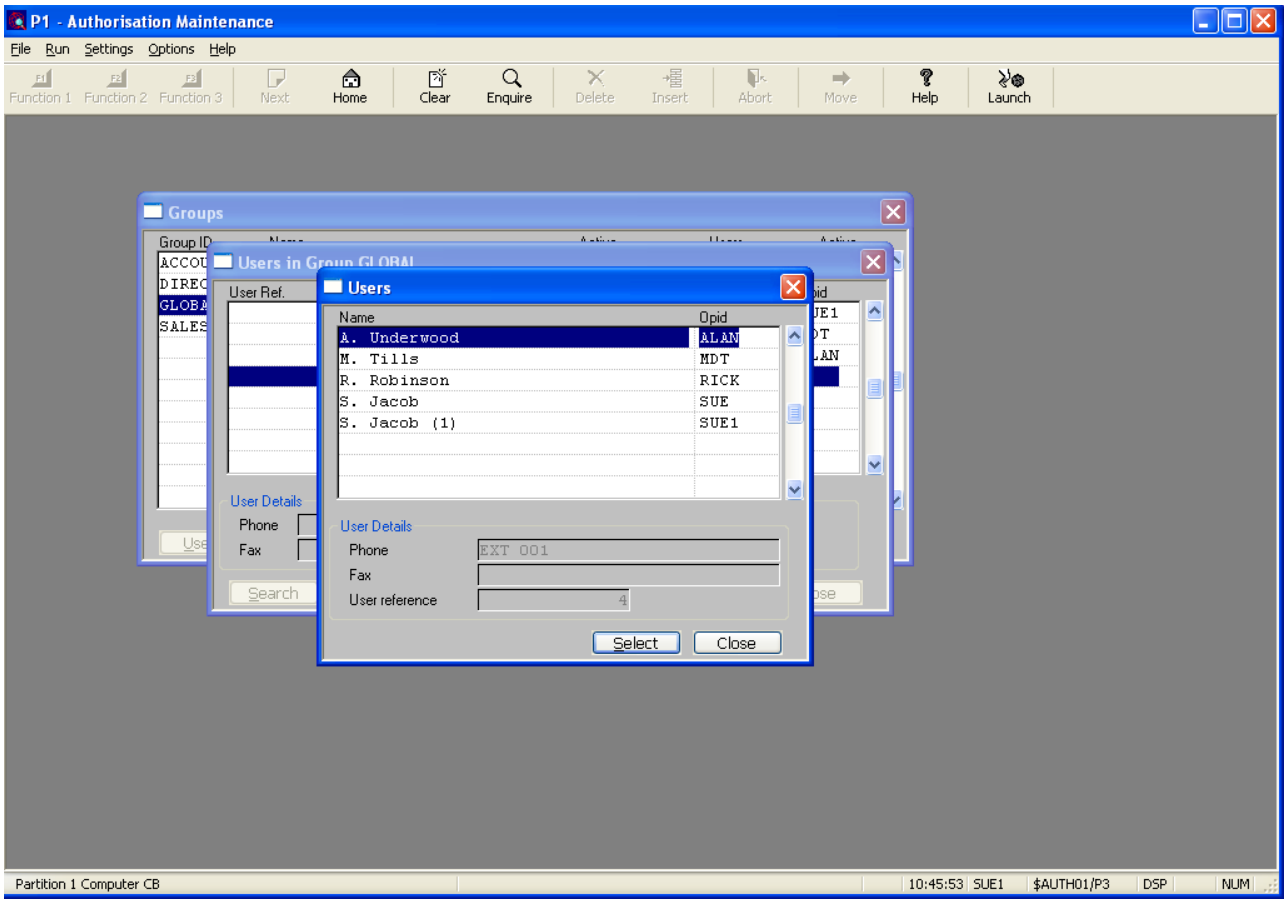
Note that you may also add users to a group from the ‘Users’ entry on the main menu.

To delete a user from the group, you must position on that user and select the ‘Delete’ button from the toolbar.

You may modify the active flag for a user in the group. Users who are not active in the group, are not considered as members of the group for access to Authorisation Points.

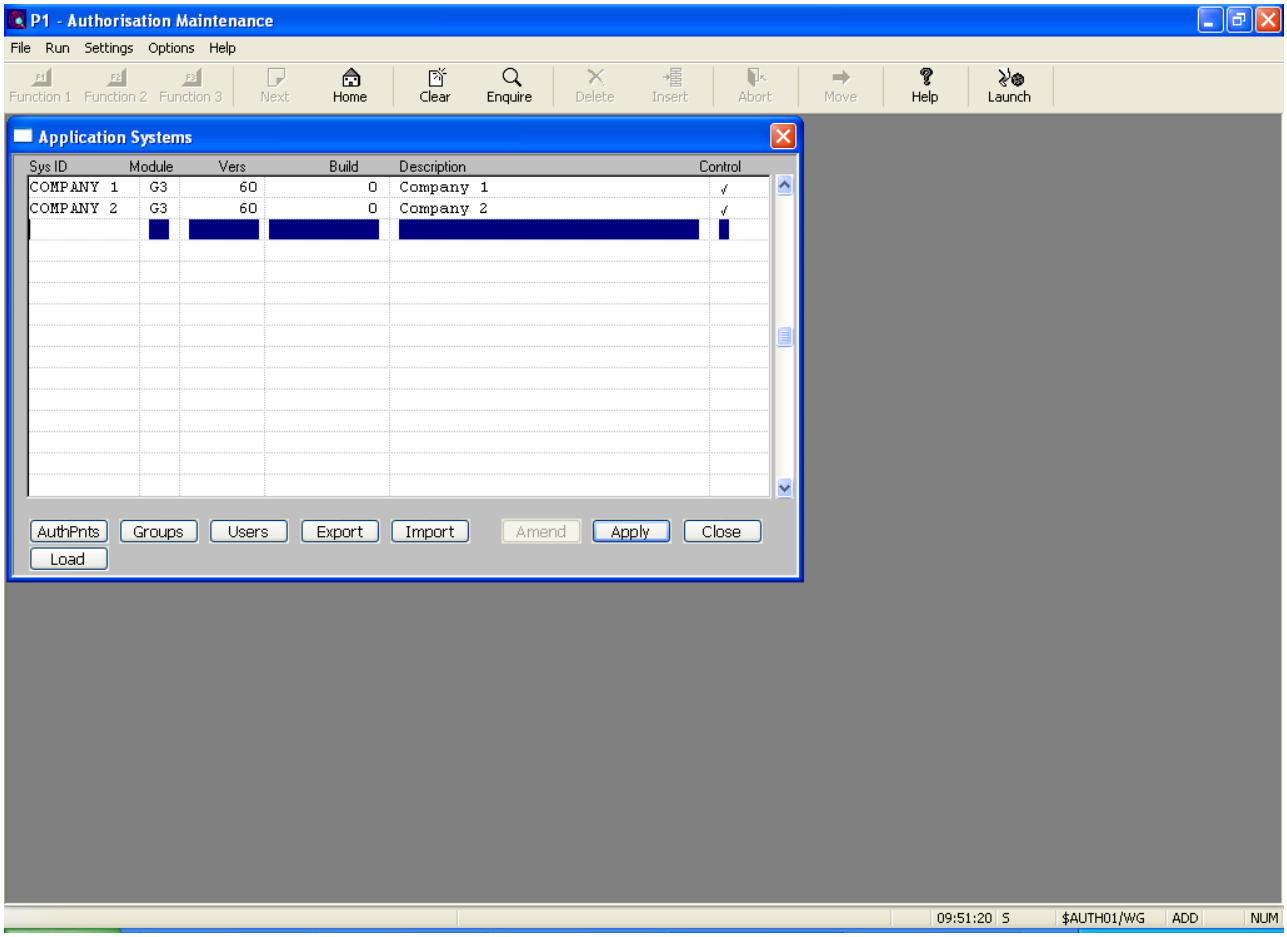
You should note that a user may not be active but can still be an active user within the group. The two active flags indicate whether a user is an active user and whether the user is active within the group.

To add a user to the end of the list you must key the user reference number. To list the current users and to select one press the ‘Search’ button on the window



4.3 Application Systems

To modify access to application system Authorisation Points you must select ‘Application Systems’ from the main menu.



System/module combination must be entered here before their Authorisation Points can be merged into the authorisation database by actually running the application, or for GSM SP-24 or later, by using the Load button. If they are not entered no application points will be merged.

The list of existing system/module combinations are shown. The build number is an indication of the last upload of Authorisation Points for the specified system/module combination. If the build number is set to 0 then no Authorisation Points have been loaded.

The description and control flag may be modified. The control flag indicates that you wish to control access to the system/module combination.

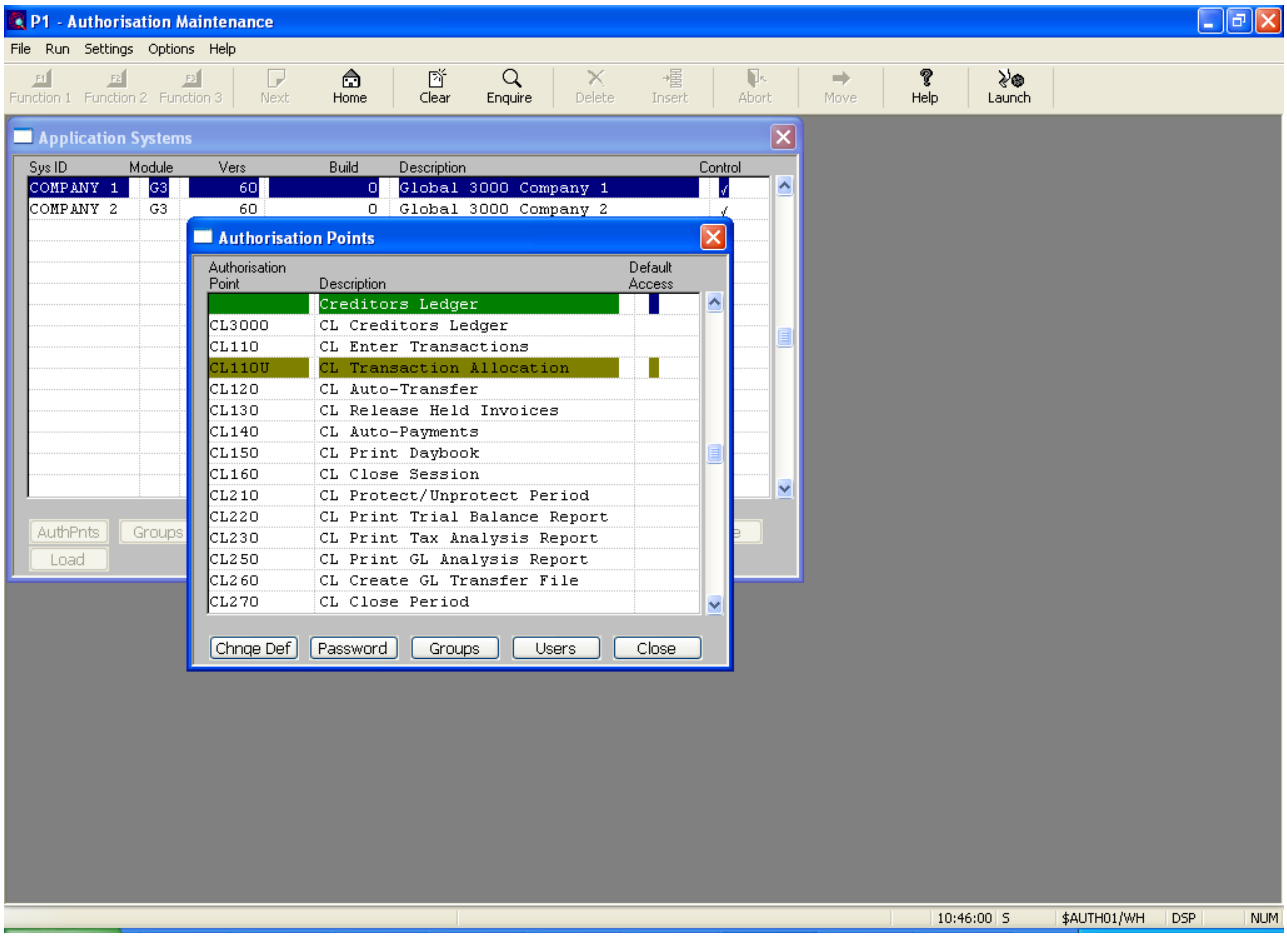
You may add a new system/module combination to the end of the list or insert one by selecting the 'Insert' button from the toolbar.

You may delete an entry by positioning on the line and selecting the 'Delete' button from the toolbar.

You may amend aspects of the access to the system/module combination by positioning on the entry and pressing the appropriate button.

4.3.1 AuthPnts

Pressing this button from the application systems screen will display the Authorisation Points currently loaded for the system/module combination. For entries where Authorisation Points have not been loaded this button will be unavailable.



Some entries in the authorisation point list have blank authorisation points. These are for descriptive purposes only, and are often used as headings or to separate different classes of authorisation points. These entries cannot have their 'default access' modified and are not authorisation points within the application. Colour may have also been used by the application to indicate different grouping. Please refer to the application documentation for information on the use of colour for authorisation points.

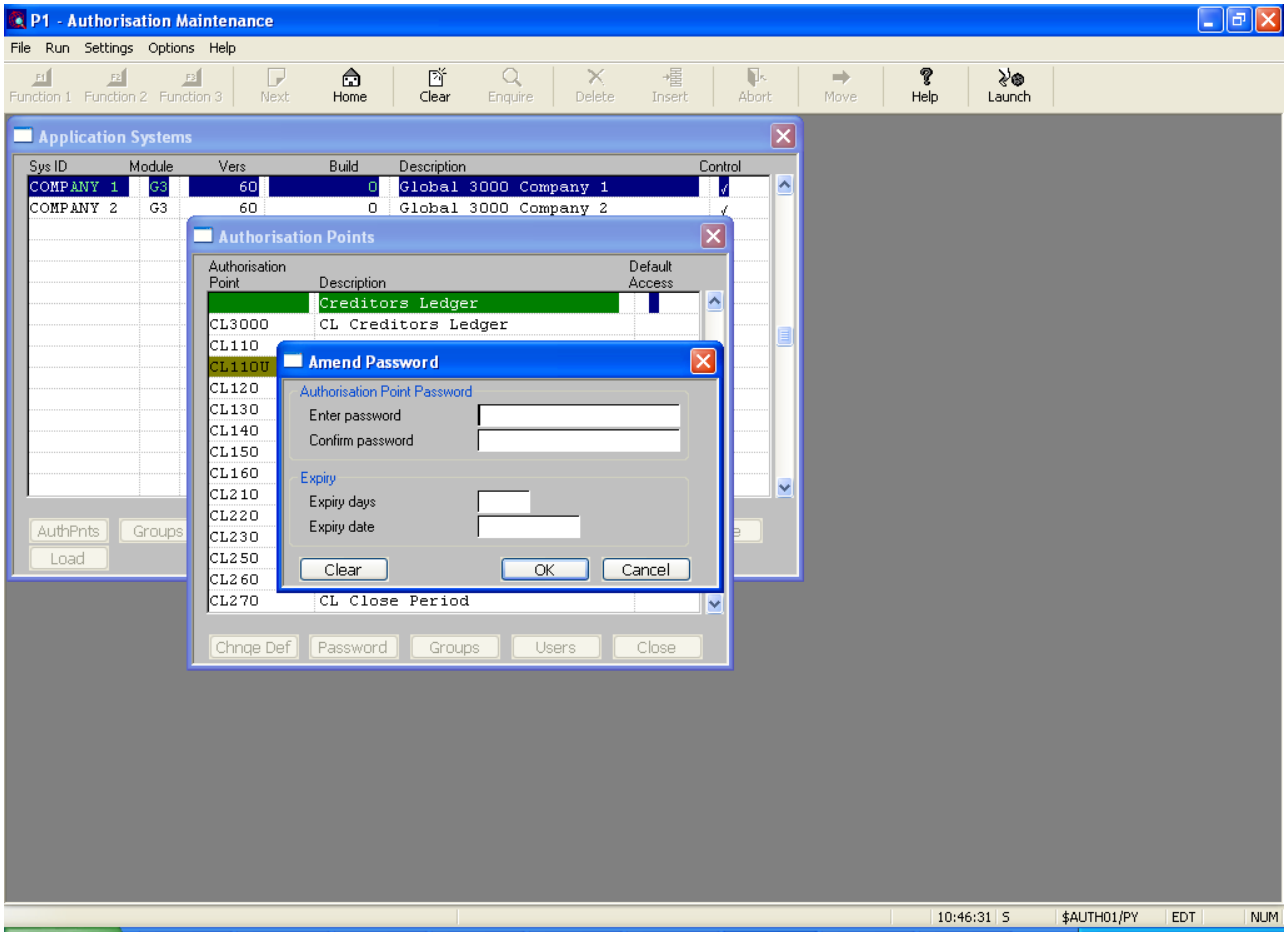
You can now amend details for a particular system/module/Authorisation Point combination by positioning on the required entry and pressing the selected button.

4.3.2 Chnge Def

This allows you to change the default access to this system/module/Authorisation Point combination to either allow or deny access. An override to this default access can be issued for either a particular user or a particular group (see later).

4.3.3 Password

You may associate a password with a particular system/module/Authorisation Point combination. This will cause the user to be asked to enter the password when attempting to gain access to this Authorisation Point within the application:



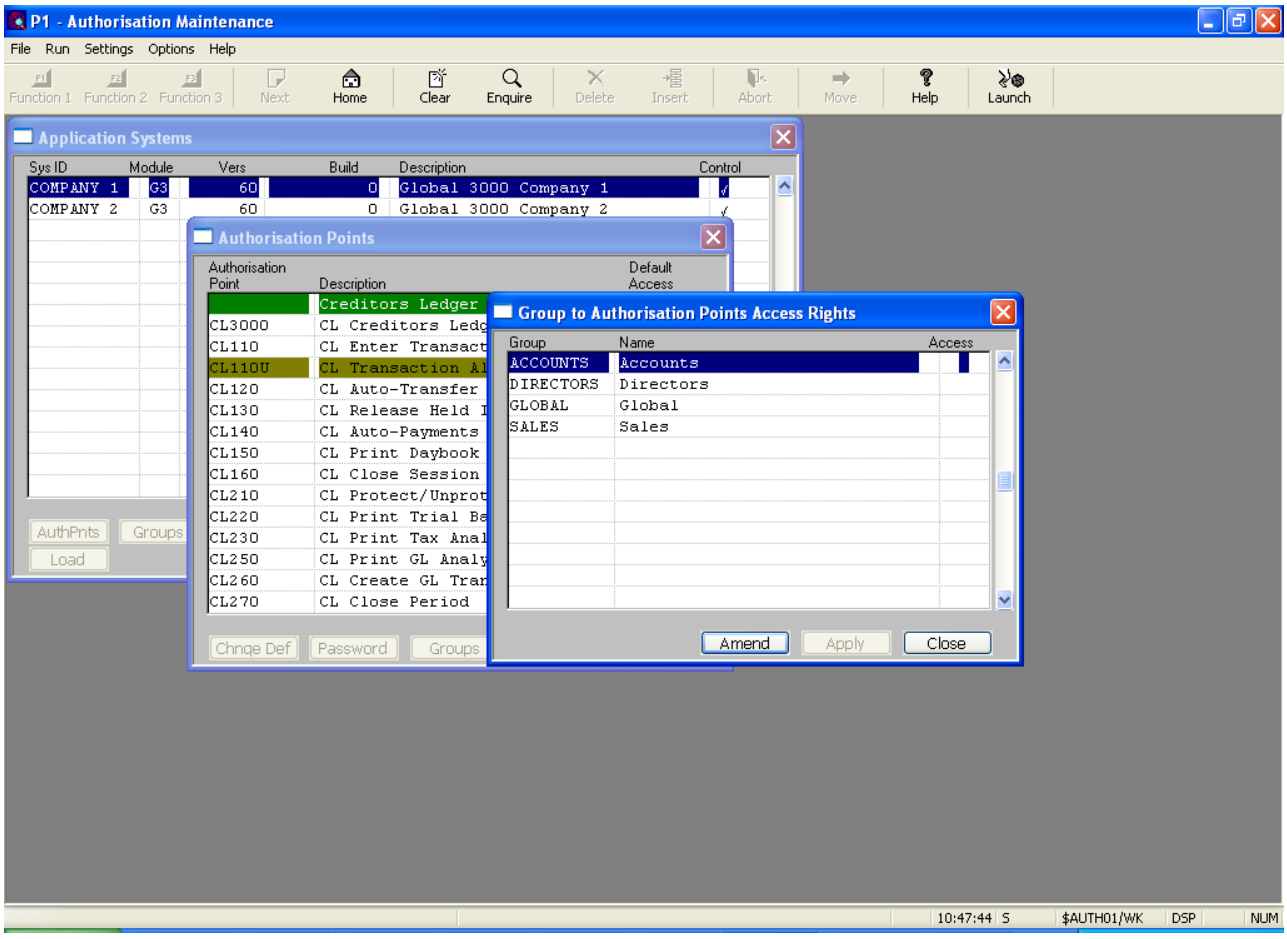
You must also enter an expiry time in days for the password. If the password for this Authorisation Point expires, $AUTH32 will have to be run to set a new password.

From GSM SP-26 the prompt will appear as ‘Enter password’ if there is no existing password, and as ‘Change password’ if there is an existing password.

Pressing the ‘Clear’ button on the window removes the password on the Authorisation Point.

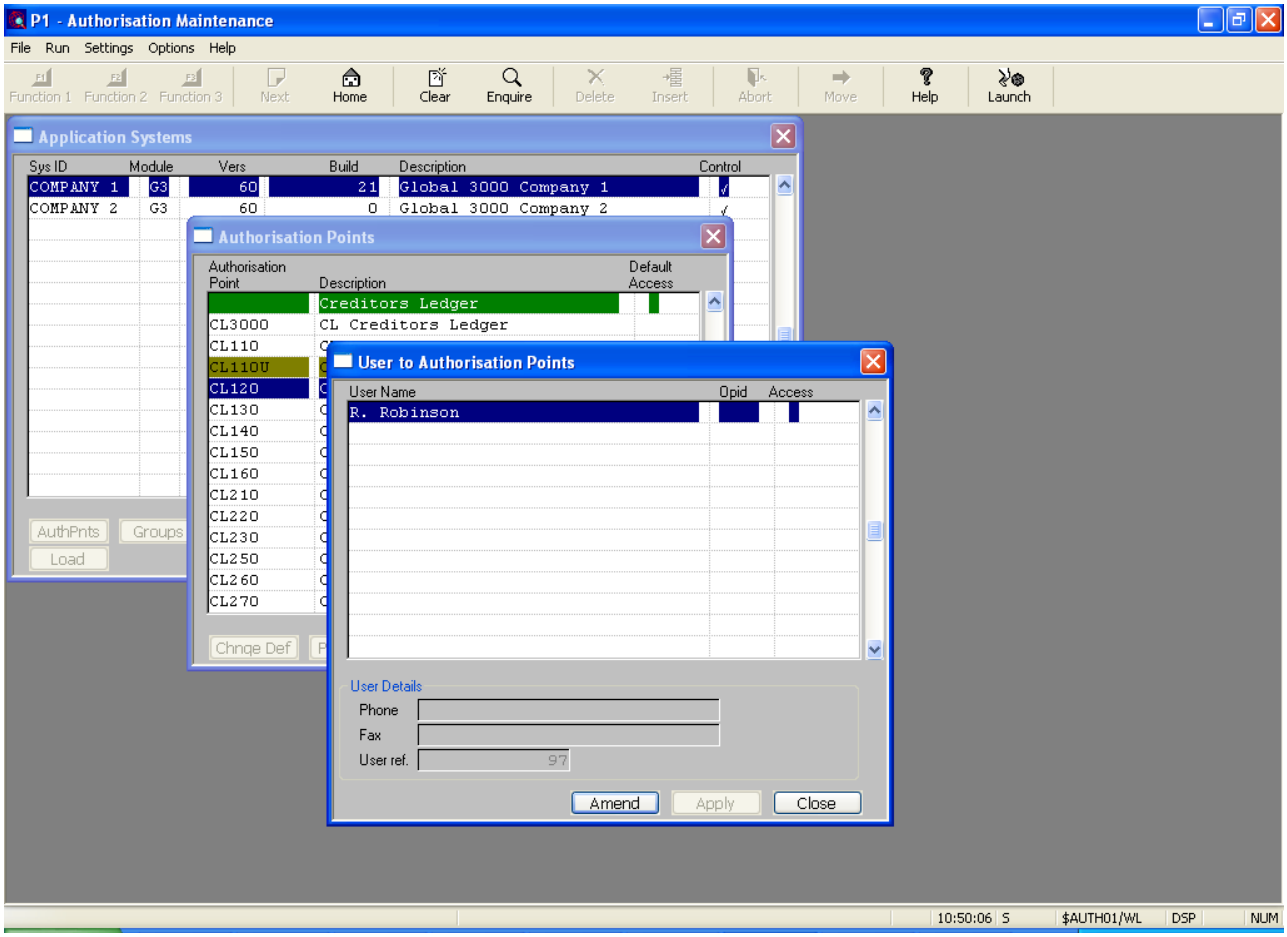
4.3.4 Groups

The ‘Groups’ button from the Authorisation Points window allows you to override the default access to the system/module/Authorisation Point, for a particular group.



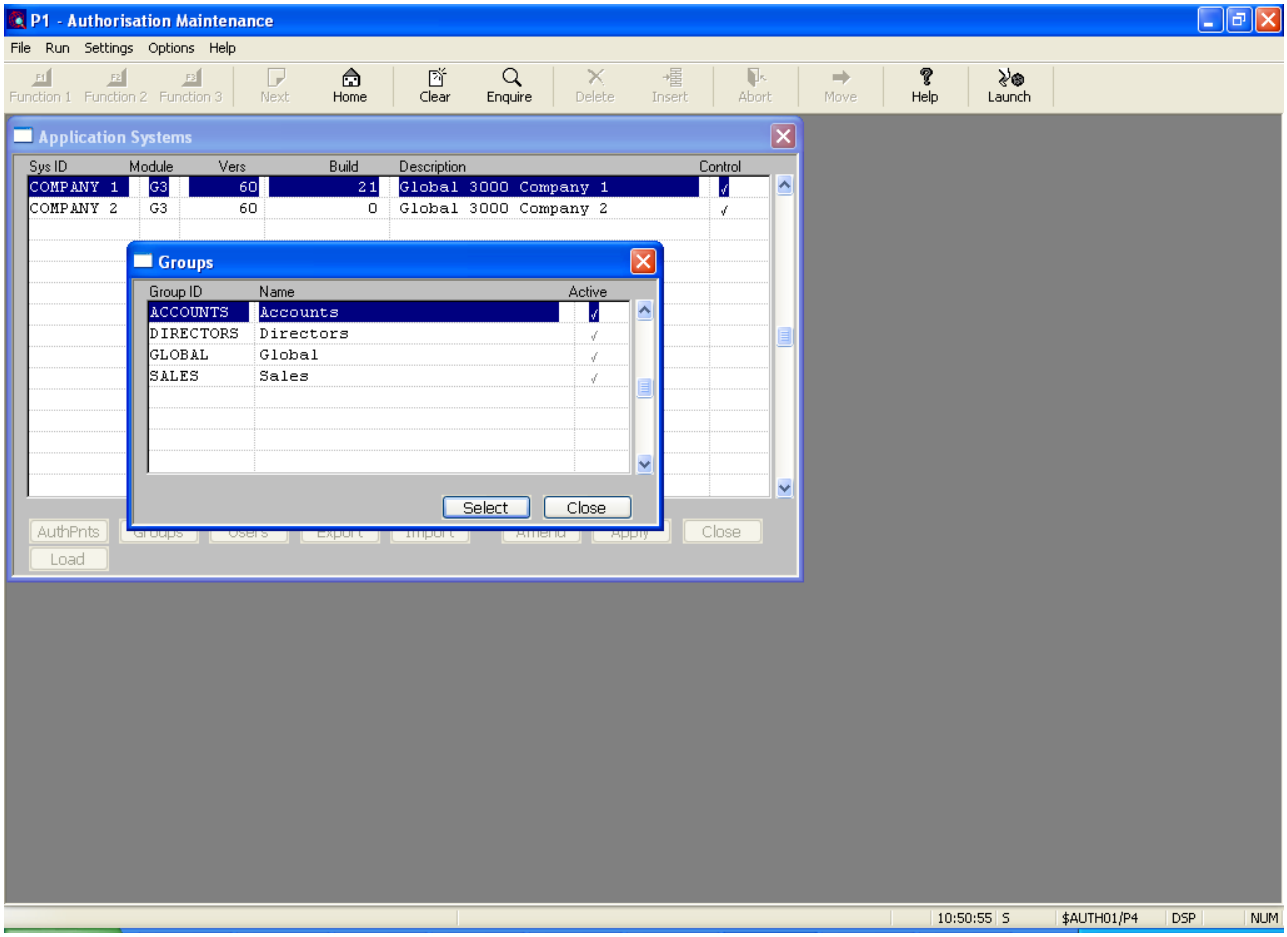
4.3.5 Users

The ‘Users’ button from the Authorisation Points window allows you to override the default access for the particular system/module/Authorisation Point combination for a selected user. The users shown are those for whom the system/module combination has been associated. To associate a system/module combination to a user you need to select the ‘Users’ option from the main menu.

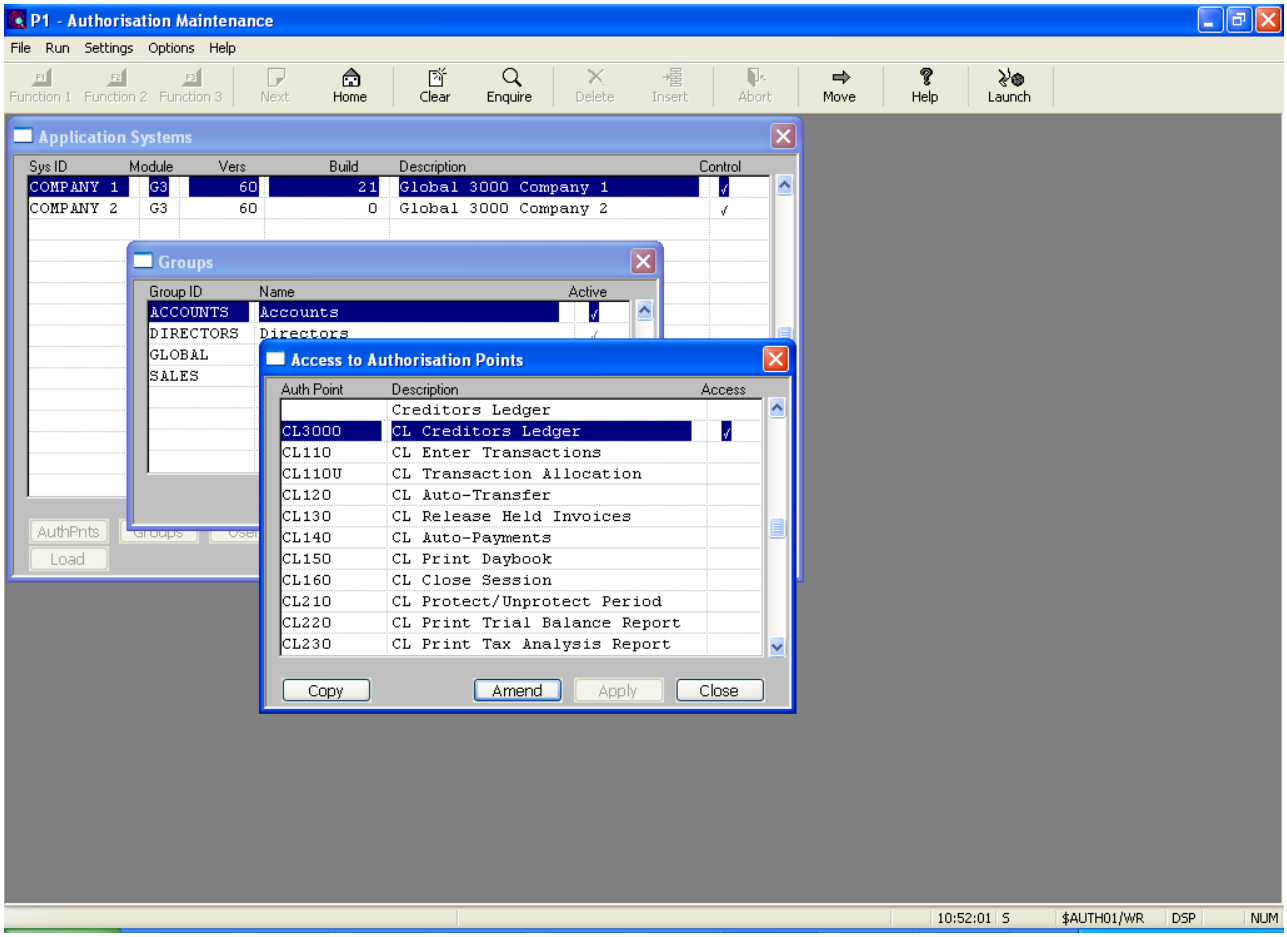


4.3.6 Groups

The ‘Groups’ button from the application systems window shows you the current list of groups.

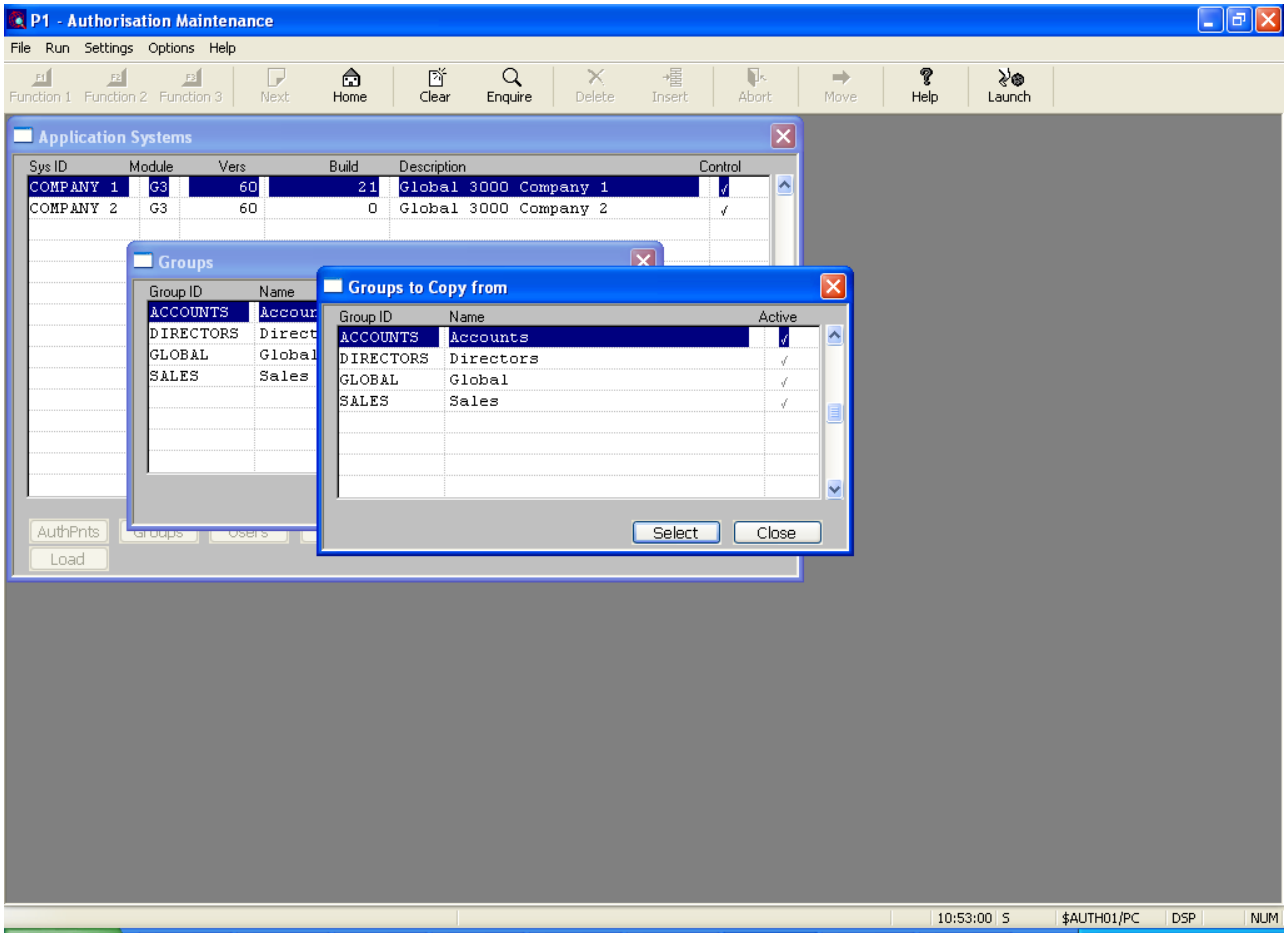


Selecting a group shows all the Authorisation Points for the system/module combination, and whether the group has access or not.



You may modify the access to the system/module/Authorisation Point and override the default access to the authorisation point. Any override value is shown in a different colour.

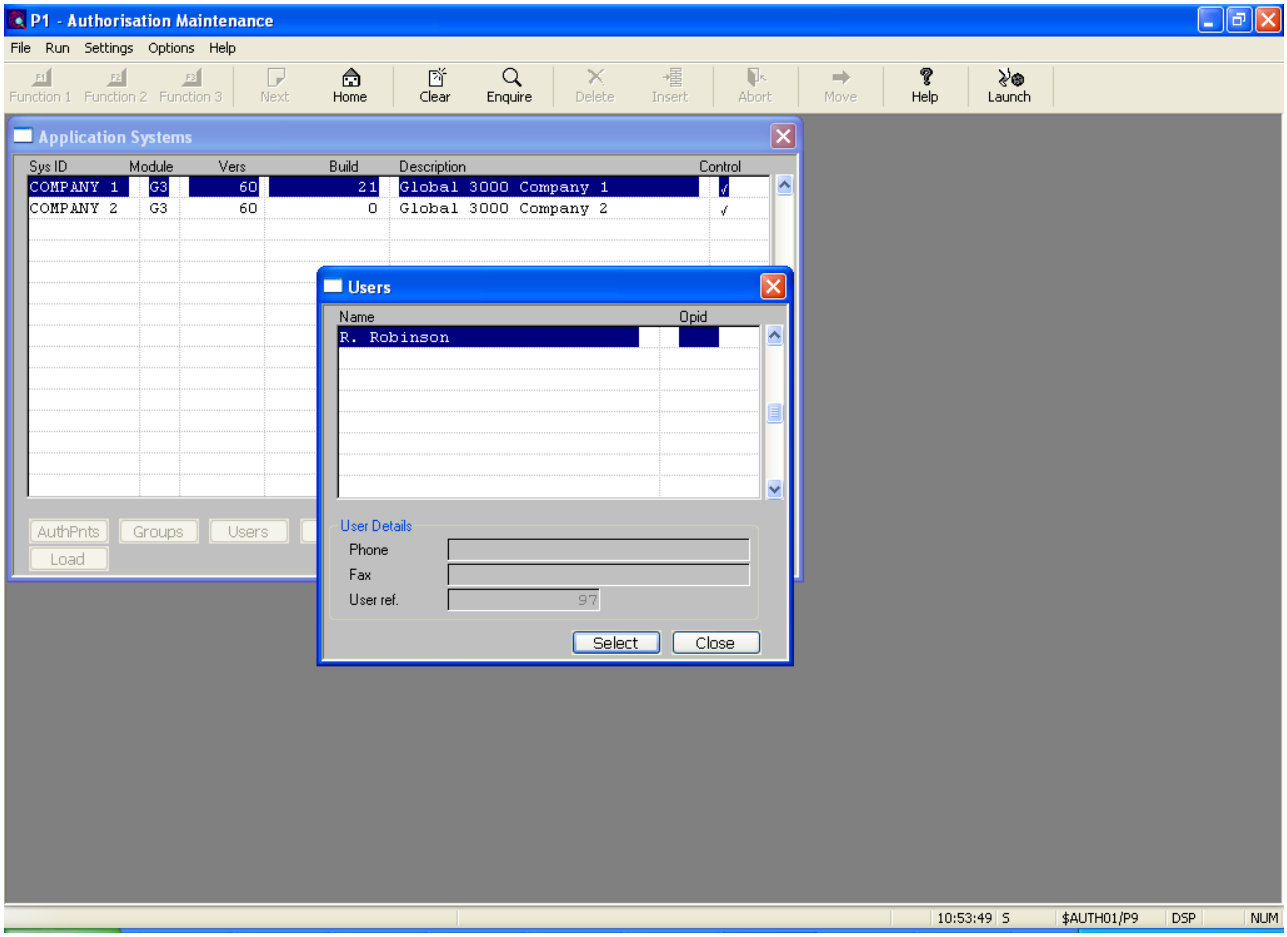
The ‘Copy’ button from this window allows you to copy the access for this group from another group. Pressing the ‘Copy’ button display the list of groups that you can copy from.



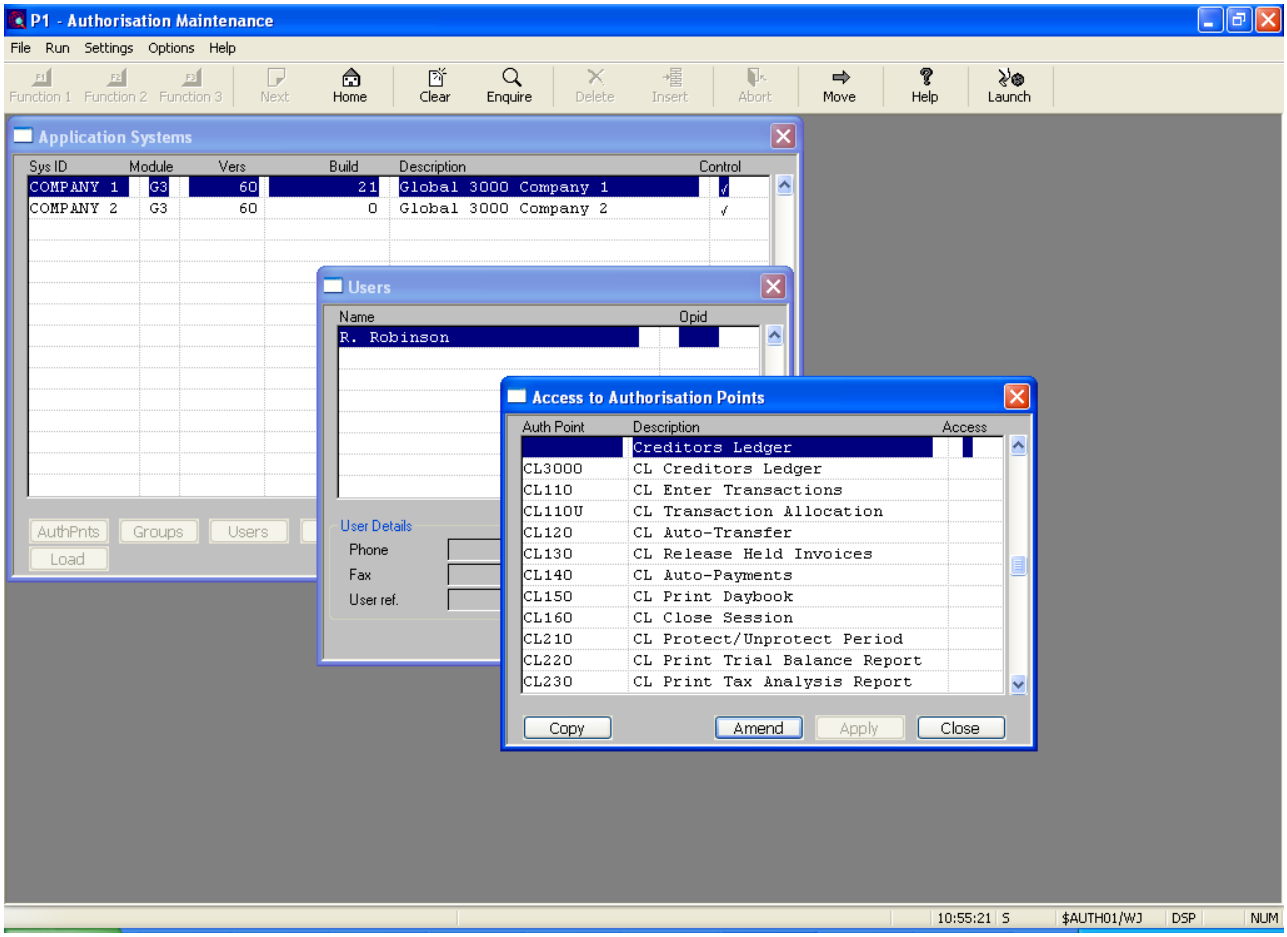
Simply select the required group.

4.3.7 Users

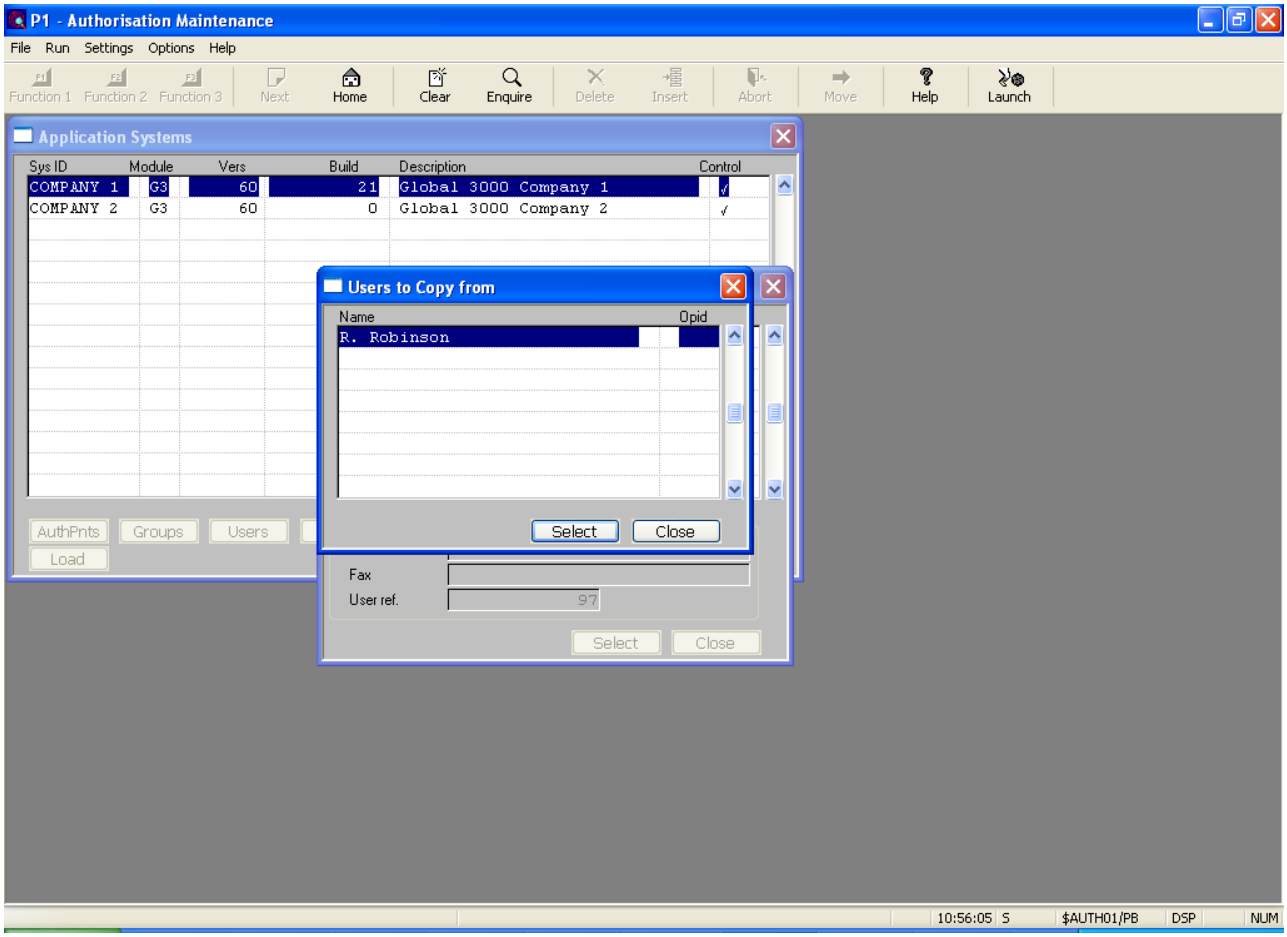
Pressing the ‘Users’ button from application systems window shows the users associated with that system/module combination. To associate a user with a system/module combination you must select the ‘Users’ option from the main menu.



Selecting a user shows the access to the system/module/Application Points for that user. You may amend the access for a particular Authorisation Point, overriding the default access. Any override value is shown in a different colour.



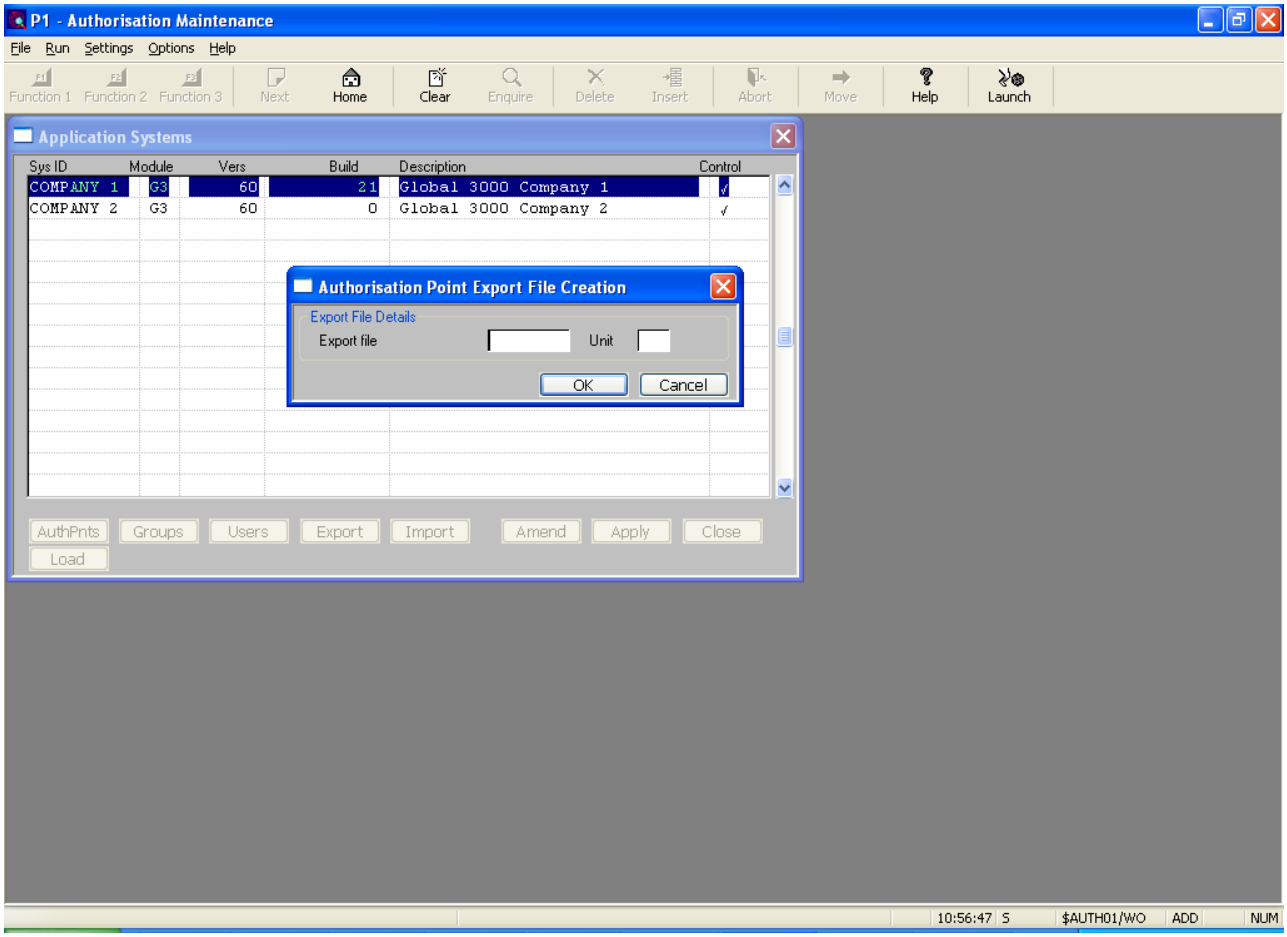
The ‘Copy’ button allows you to copy the access details from another user. Pressing the ‘Copy’ button shows you the list of users available to copy, from which you may select one.



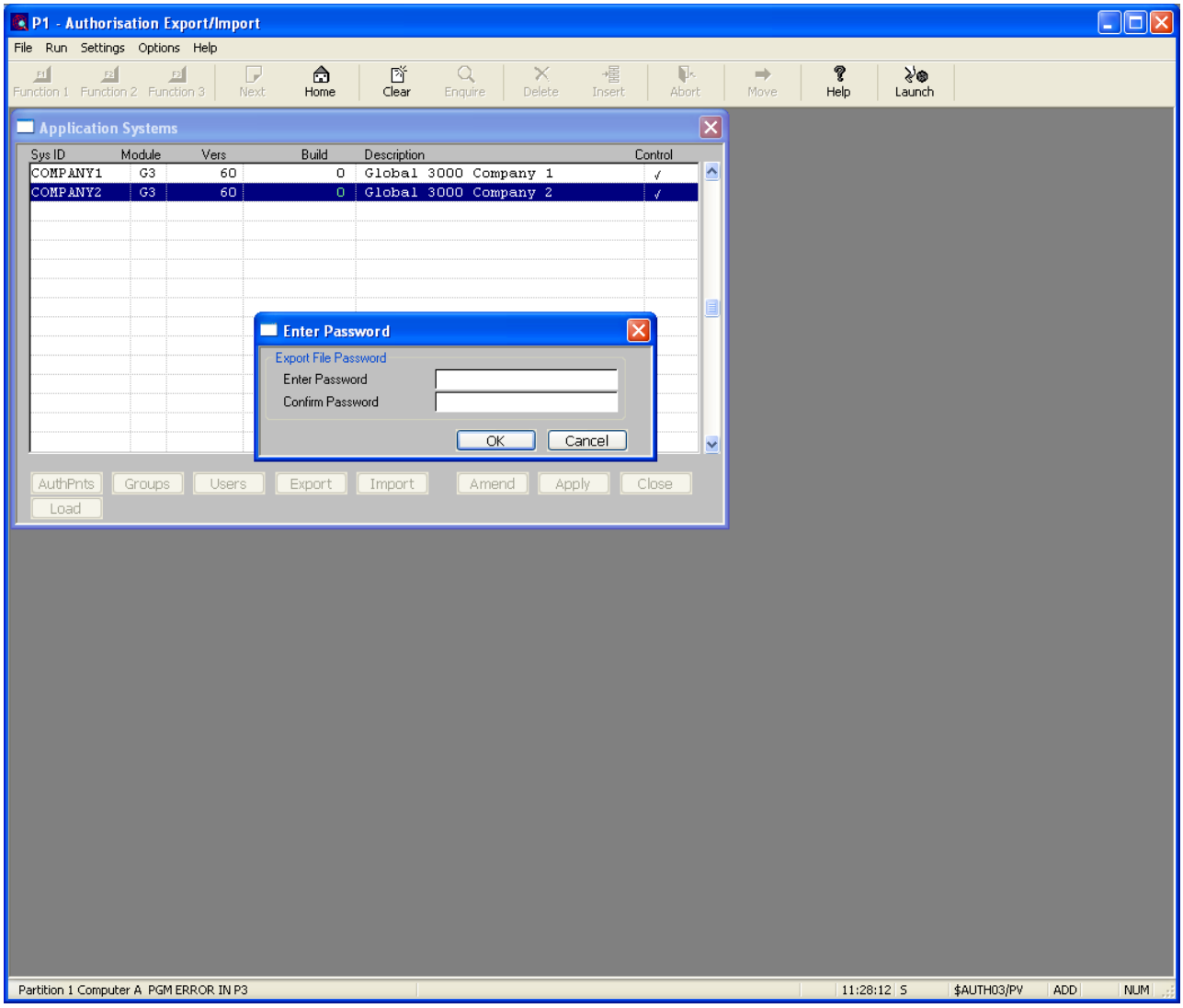
4.3.8 Export

The 'Export' button allows you to create an export file of all the system/module combinations and all its associated Authorisation Points together with the group authorisation associated with the Authorisation Points. This export file can then be imported on to another system.

The export function will ask you to enter the export file name and unit.



In GSM SP-26 and later you will also be asked for a password for the export file.

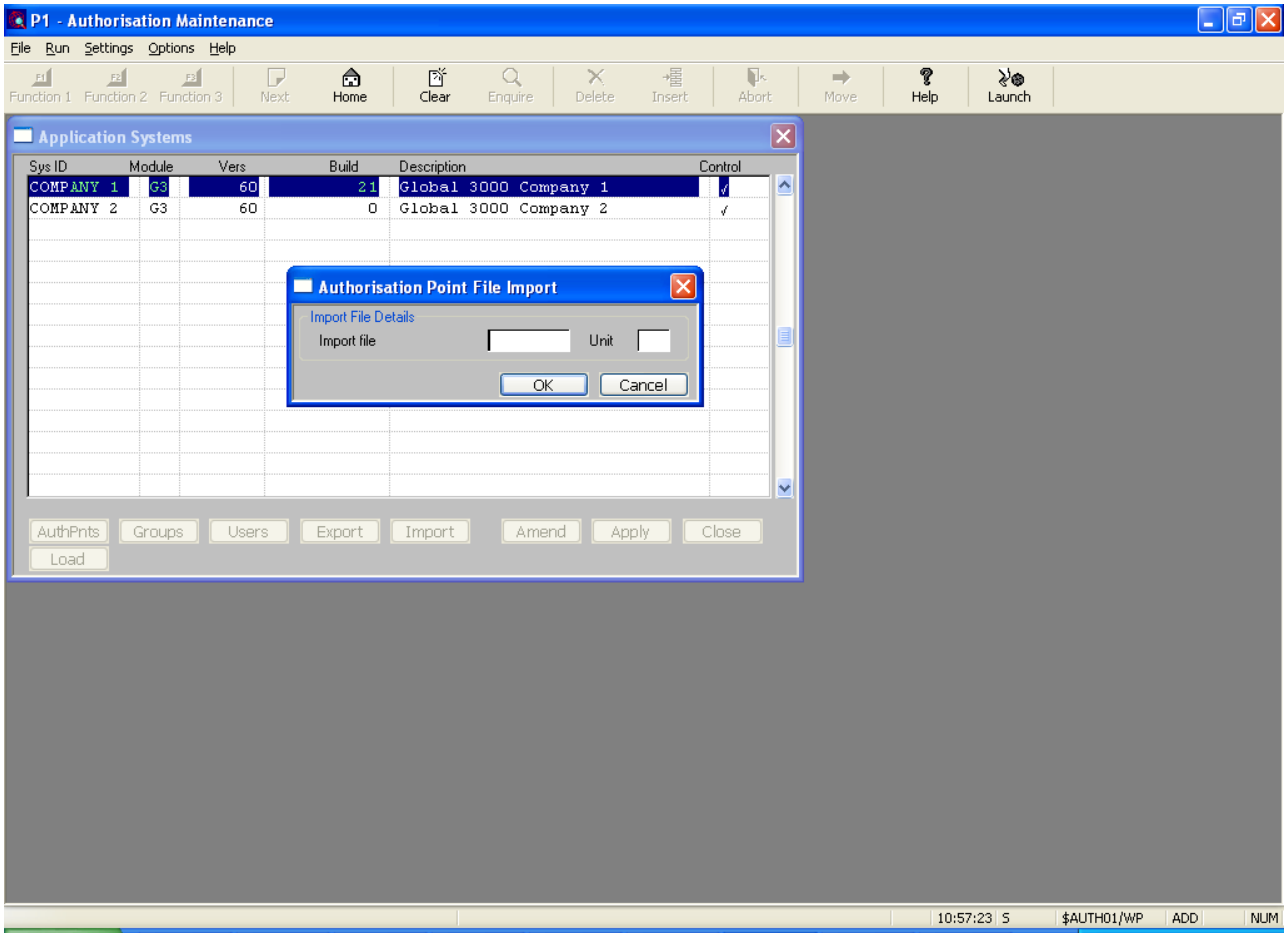


The export file will contain security information so it is advisable to set a password. This password will be required when importing this export file.

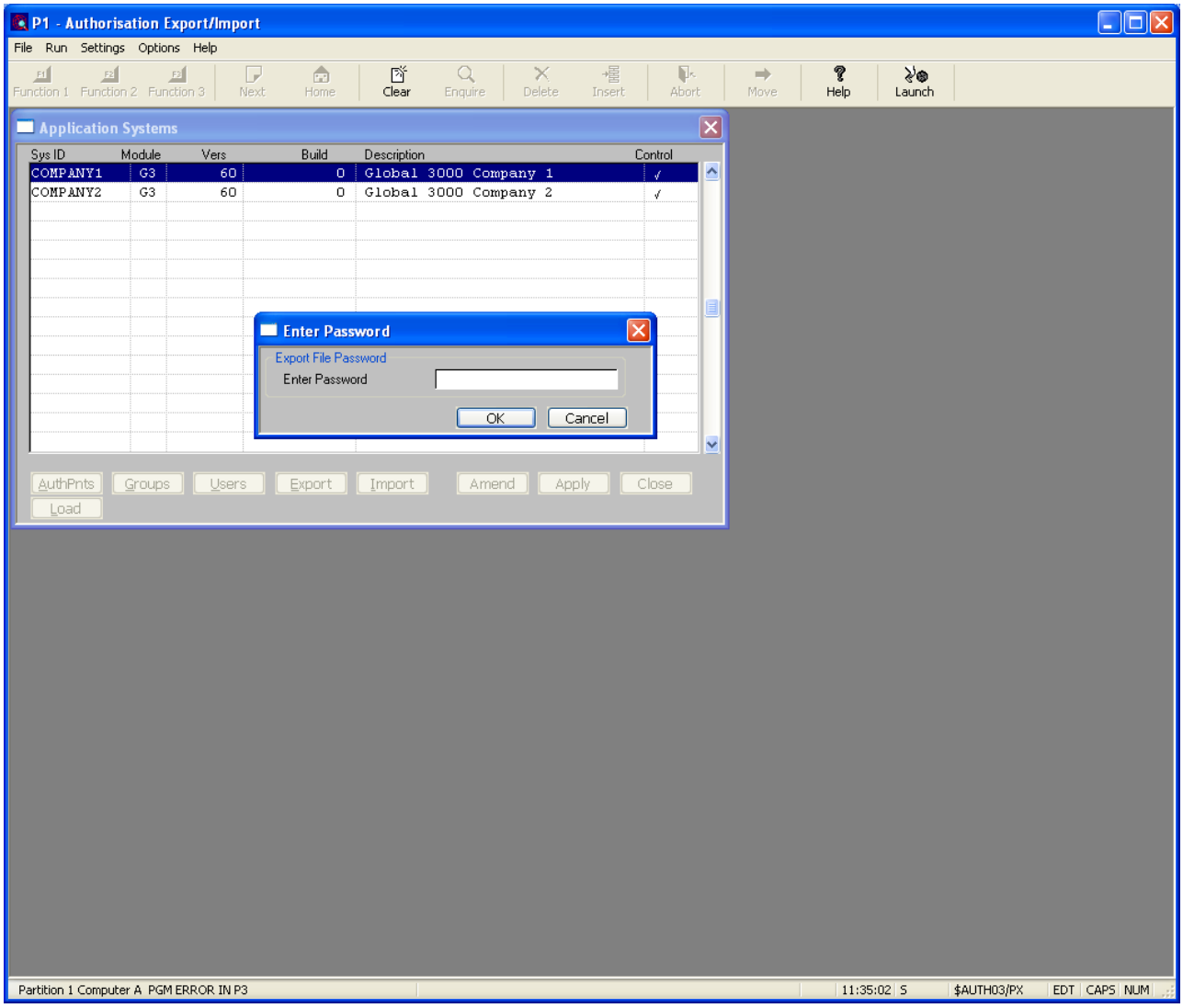
The contents of the authorisation file will then be exported.

4.3.9 Import

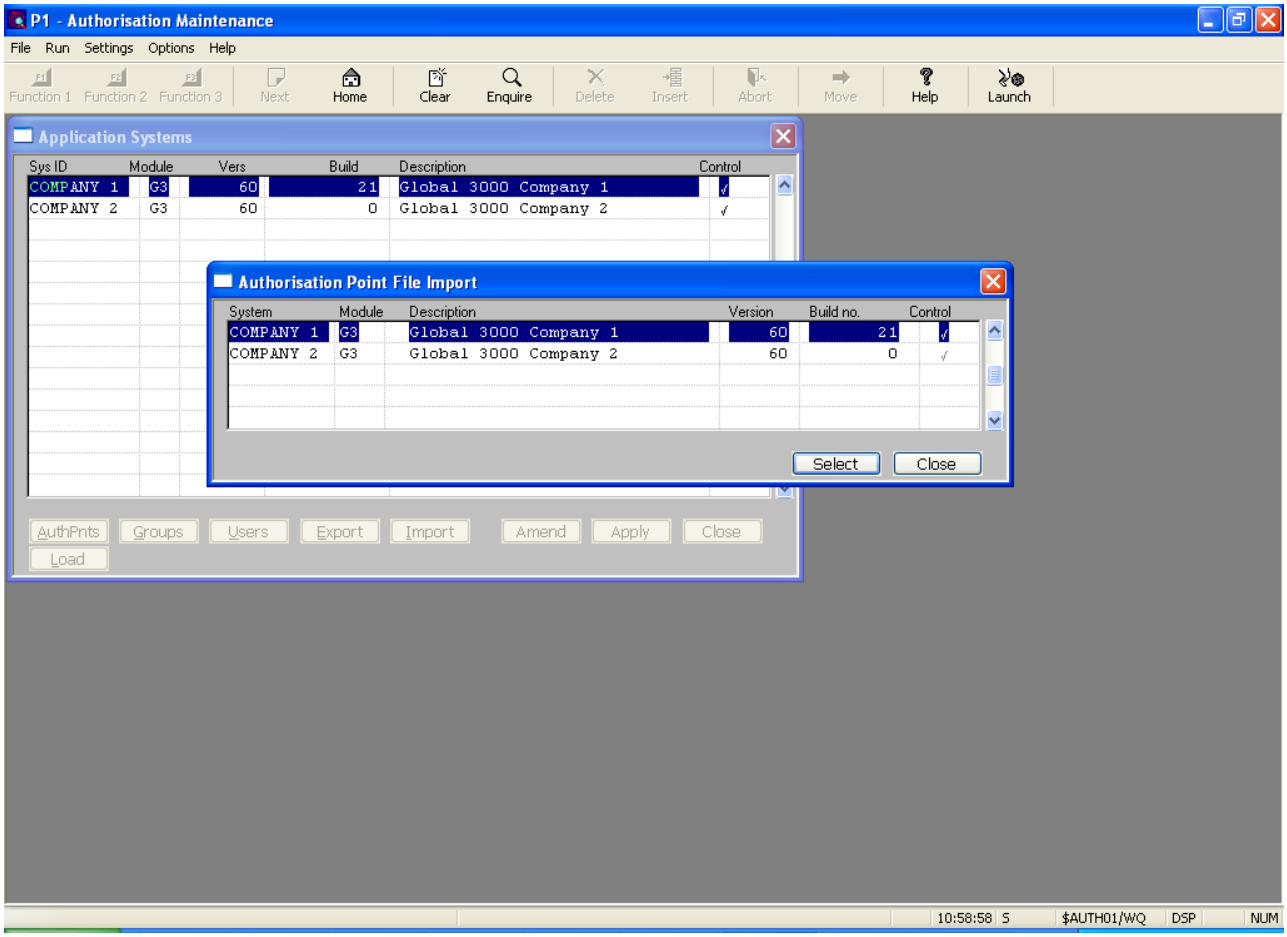
Pressing the 'Import' button allows you to import an export file. You will first be asked to enter the export file name and unit.



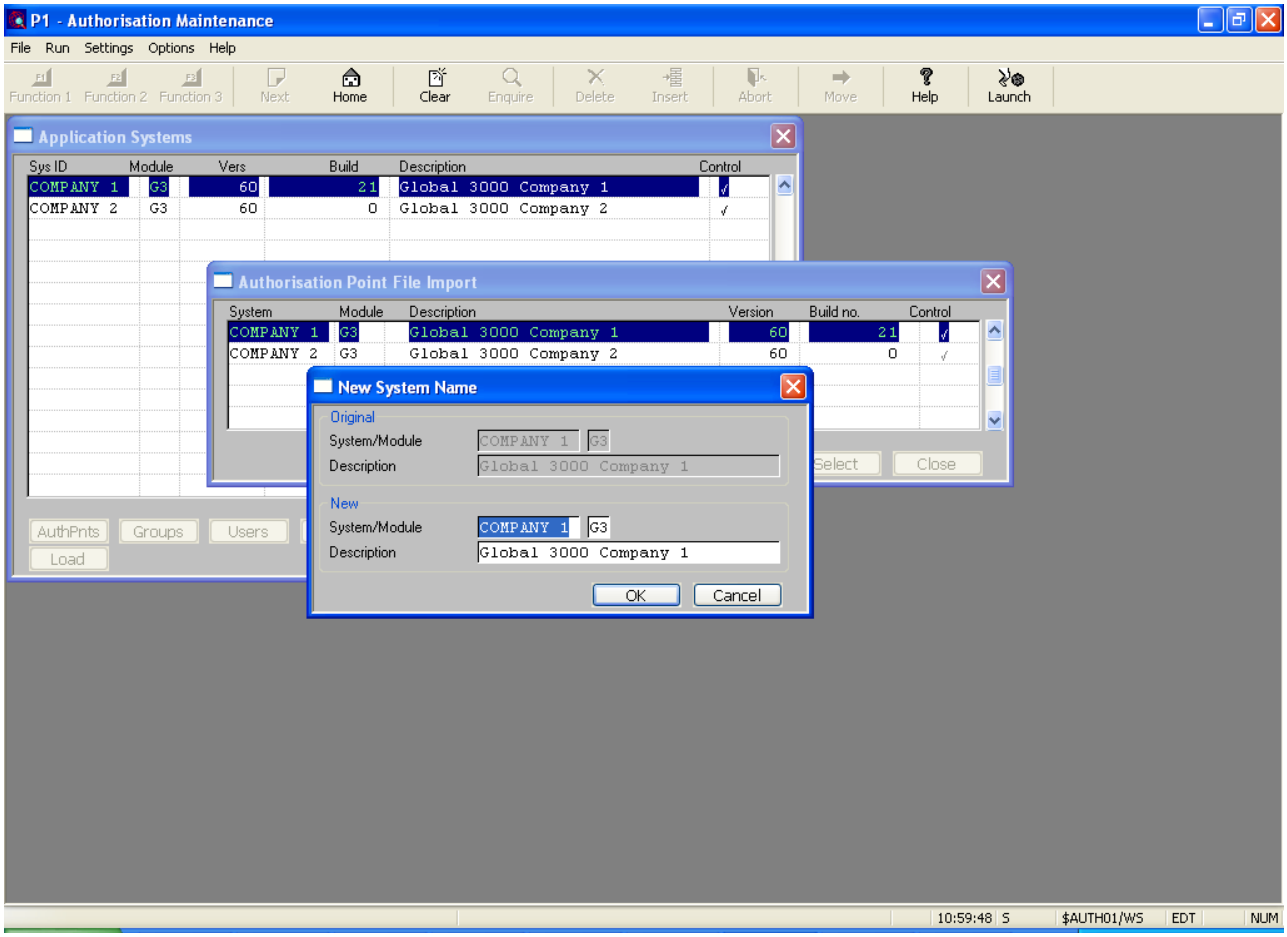
For export files created using GSM SP-26 and later you will also be asked to enter the export file password if one exists.



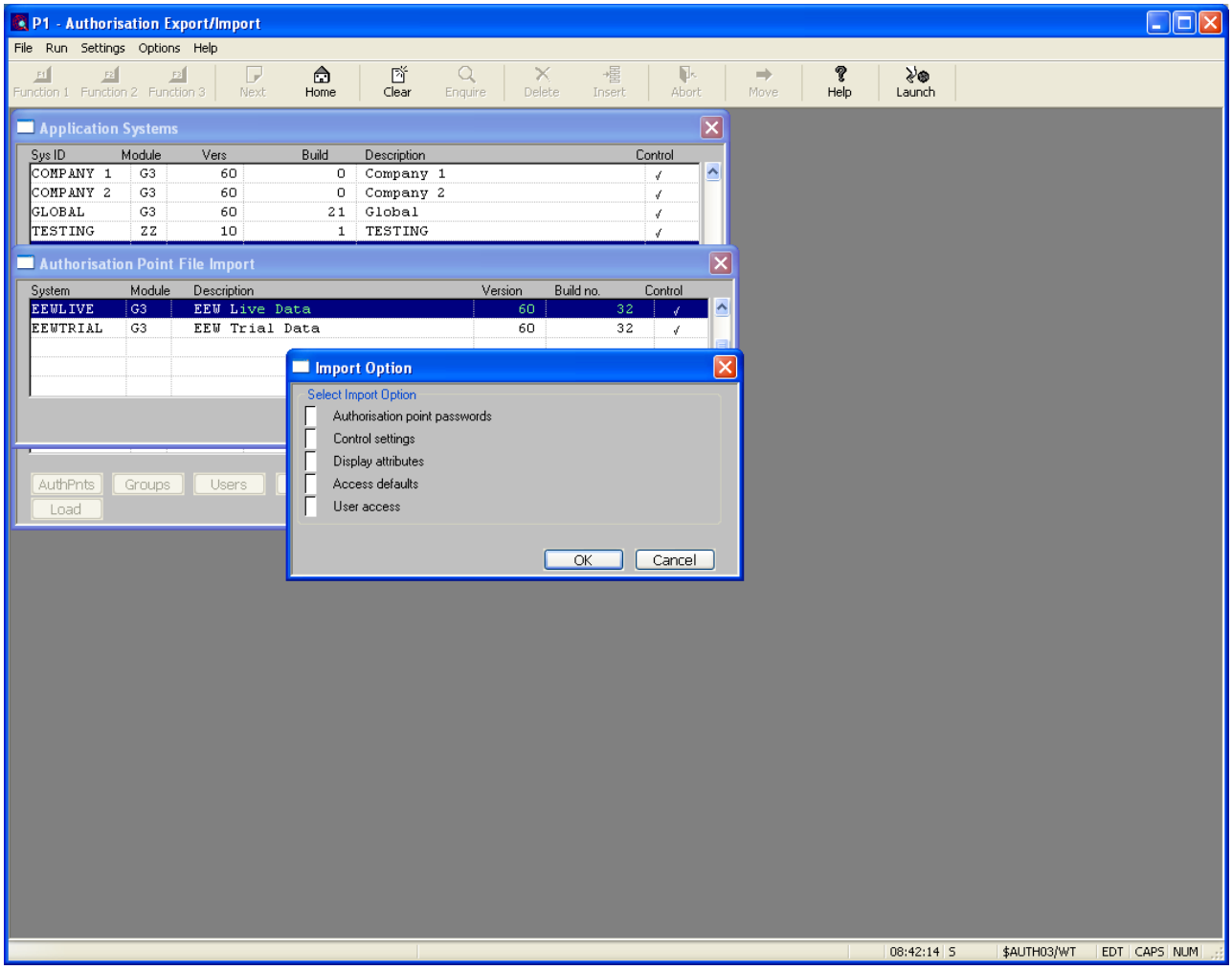
The list of system/module combinations held in the export file will be shown and you may select a system/module combination to import.



You may import the system/module to a new system/module combination by entering the new details.



For an export file created using GSM SP-26 and later you will be given the option of importing additional aspects of the system, authorisation point, user and group associations.



Authorisation Point Passwords
Provided you have not changed the original system name, you may optionally import the authorisation point passwords associated with the authorisation points in the selected system.

Control Settings
You may import the control settings for this system.

Display attributes
You may import the display attributes (colours) for the authorisation points in the selected system

Group Default
You may import the group default access information for the authorisation points in this system if they differ from the default access setting for the authorisation point.

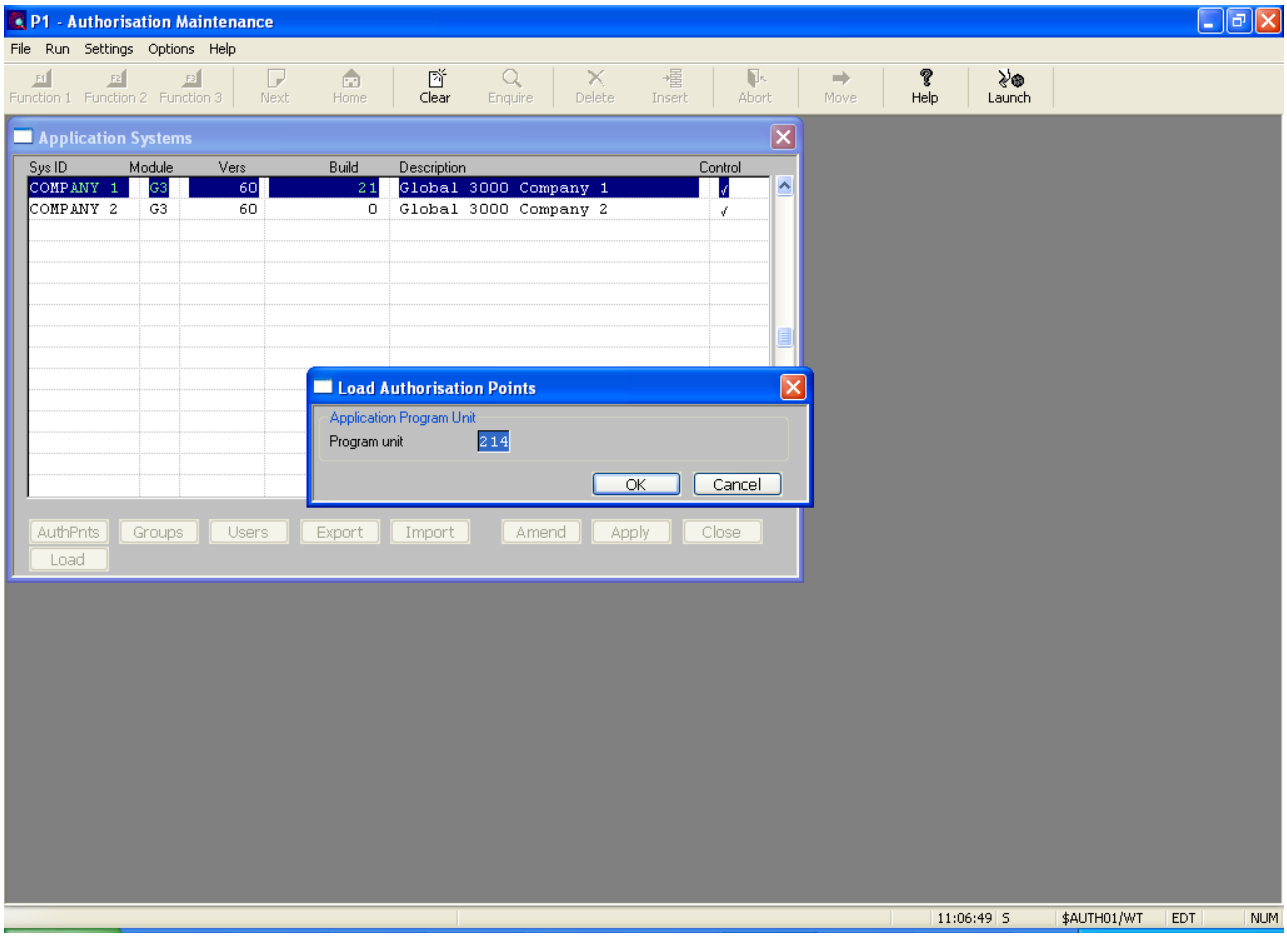
User Access

You may import the user access defaults and control information (if the contrl settings flag is set) for any operator-id that currently exists in the authorisation database.

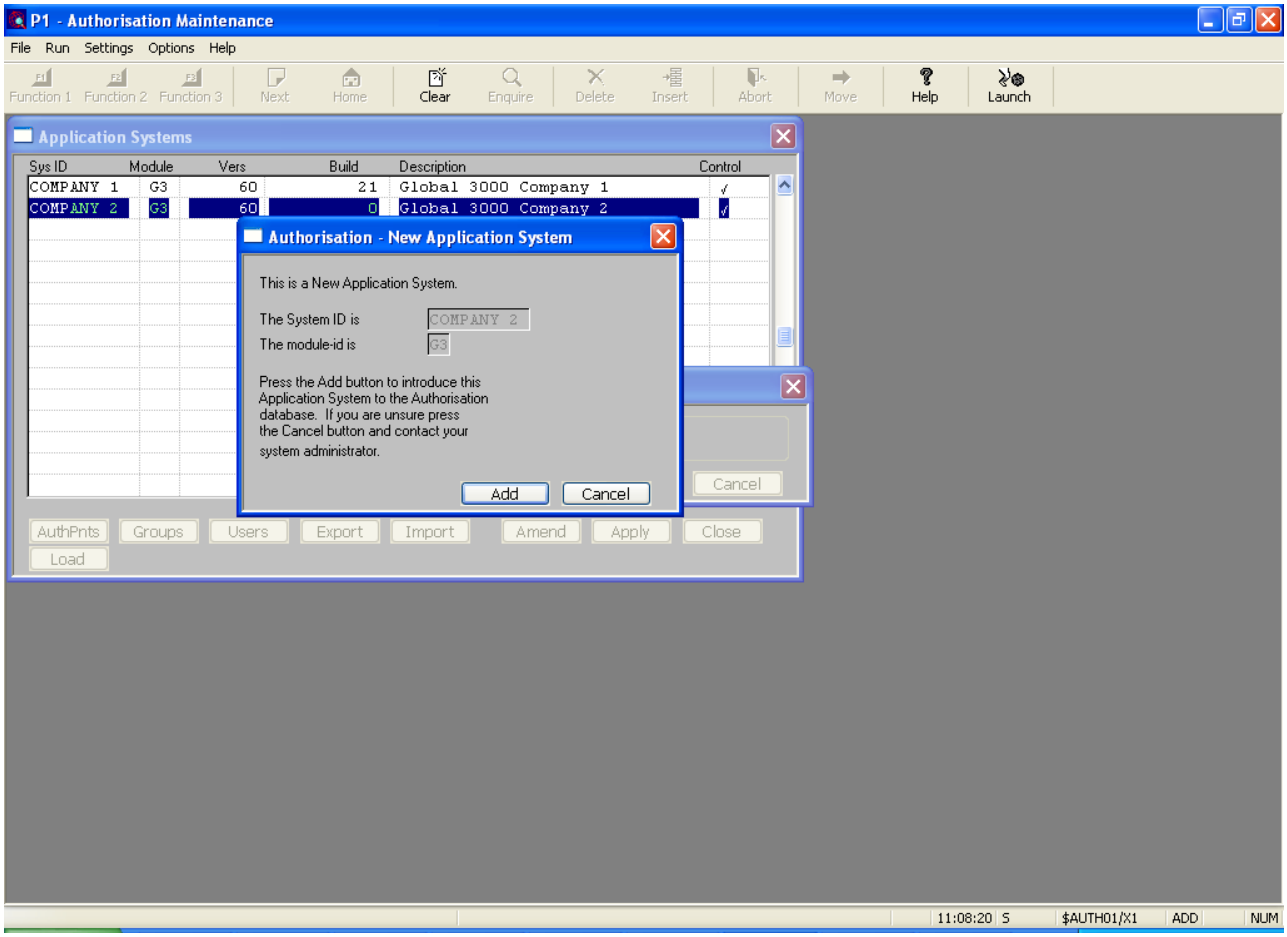
The Authorisation Points and group associations will be imported to the new system/module combination.

4.3.10 Load

For GSM SP-24 and the 'Load' button is available. This button allows you to load the application points for the selected 'System/Module' combination from the appropriate application unit. The module and version must match that on the application unit. When the 'Load' button is pressed you are asked for the application unit as follows:



A window confirming that you want to load the authorisation points will appear.

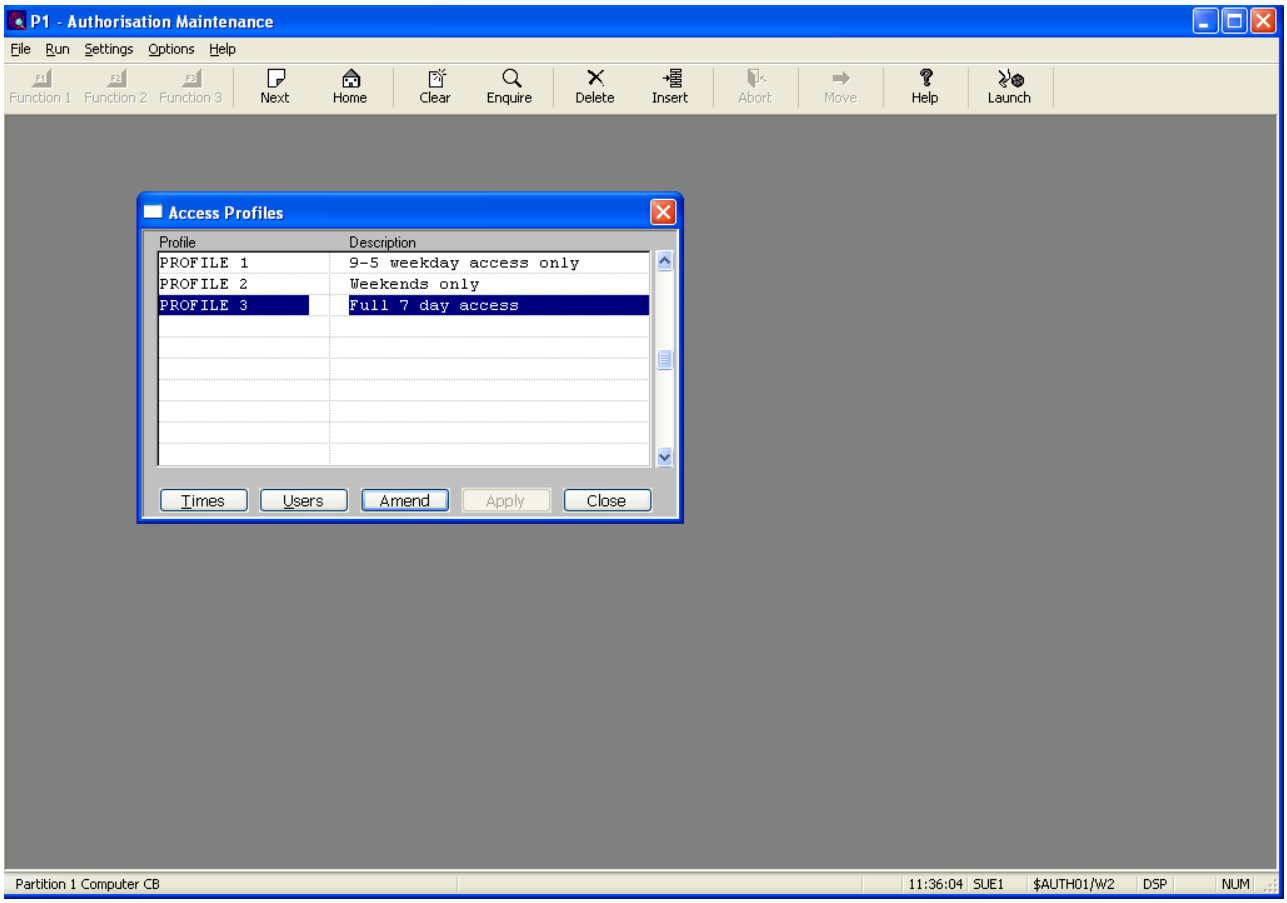


Press the ‘Add’ button to add the authorisation points to the system.

4.4 Access Profiles

Access profiles can be used to limit the access of a user to a system and can be attached to a user in the user table.

Selecting ‘Access Profiles’ from the menu shows the current list:

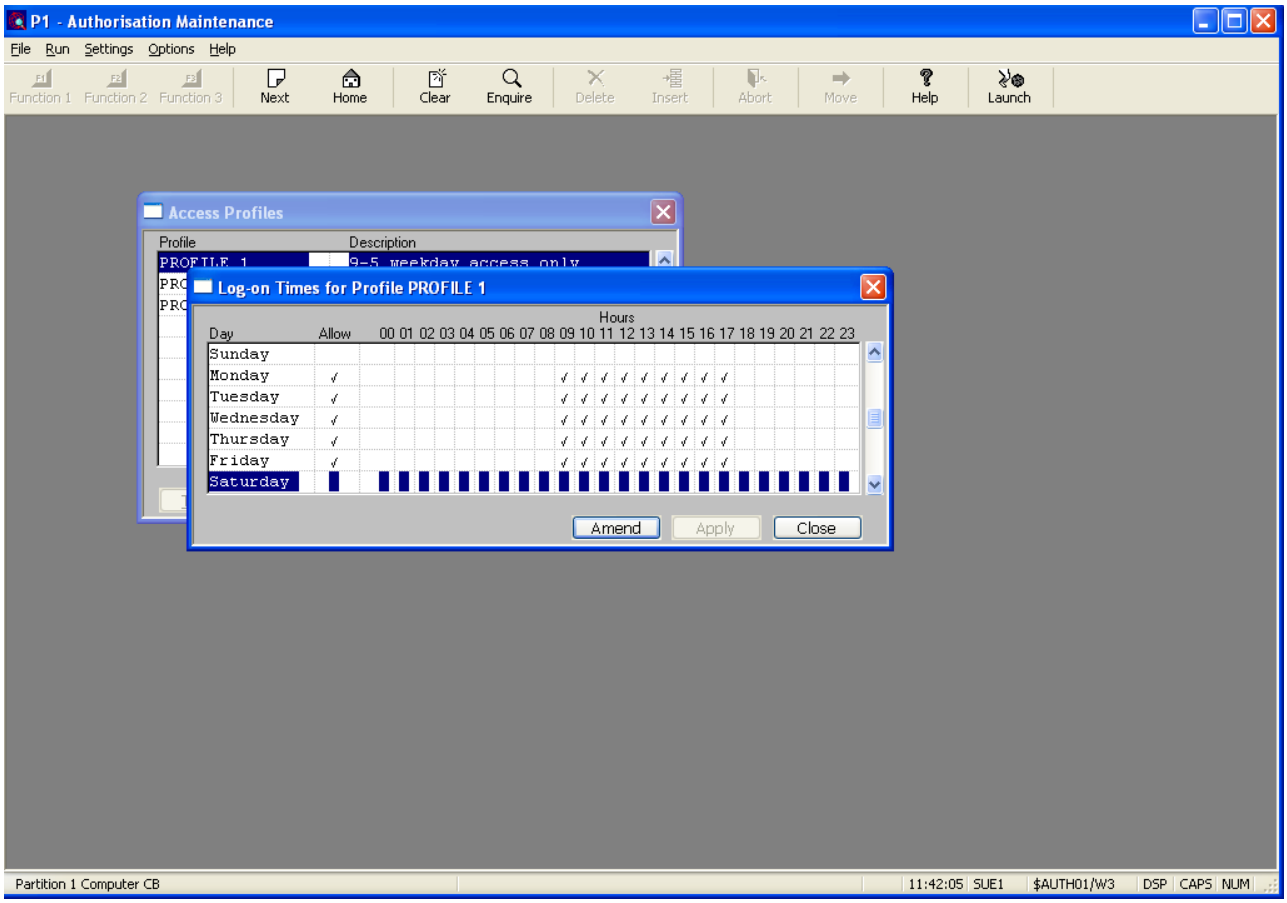


You may add new access profiles to the end of the list. You may insert a new profile by selecting the 'Insert' button from the toolbar or you may delete an entry by positioning on that entry and selecting the 'Delete' button from the toolbar.

You may amend the profile details be positioning on the selected profile and pressing the appropriate button.

4.4.1 Times

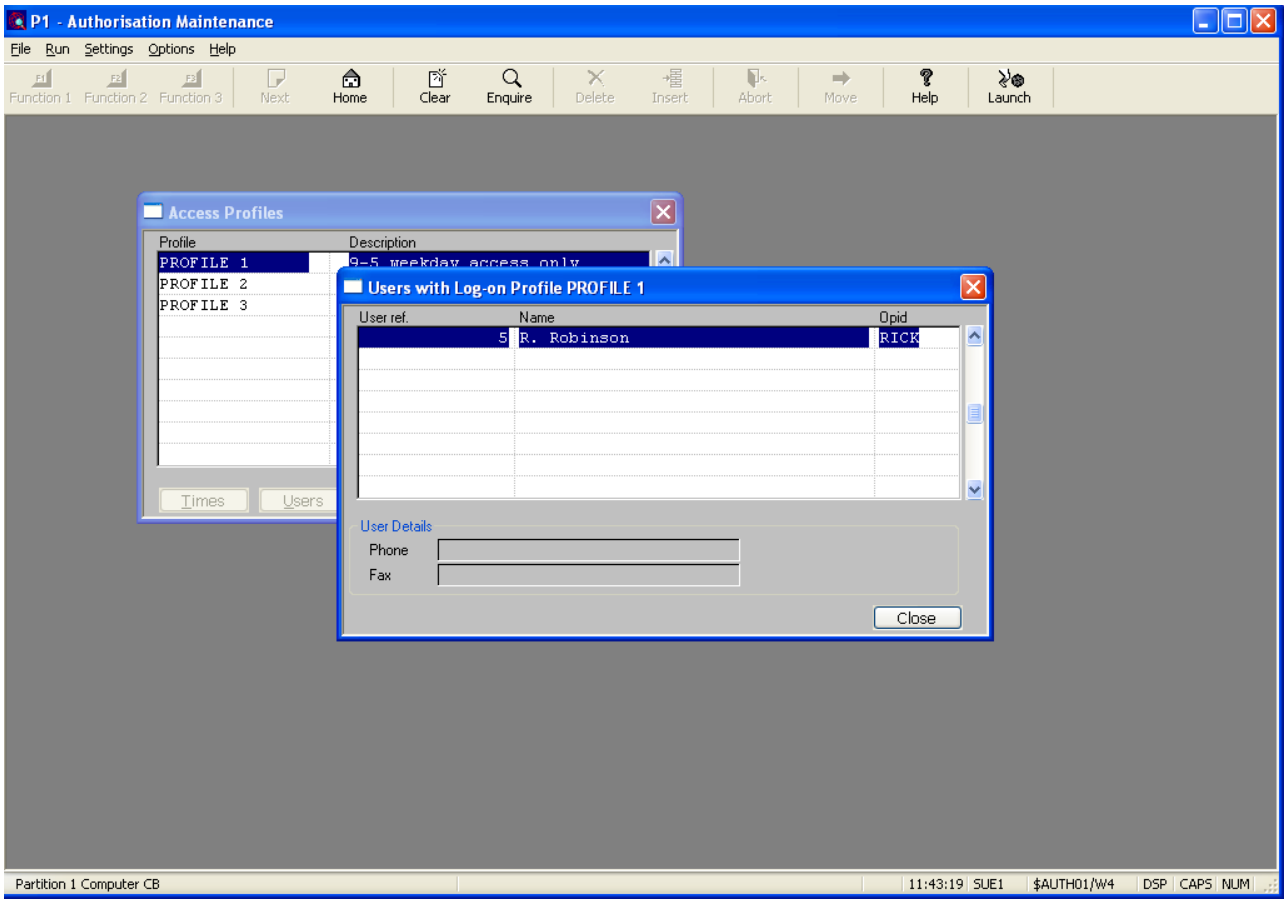
Pressing the 'Times' button allows you to amend the times for which access is allowed for this profile.



To change access for a particular day, simply clock on the ‘Allow’ column. To amend the hours for days on which access is allowed click on the appropriate hour entry.

4.4.2 Users

Pressing the ‘Users’ button on the ‘access profile’ window shows the operators currently using this access profile.



If you want to add this profile to another user you must select the ‘Users’ option from the menu.

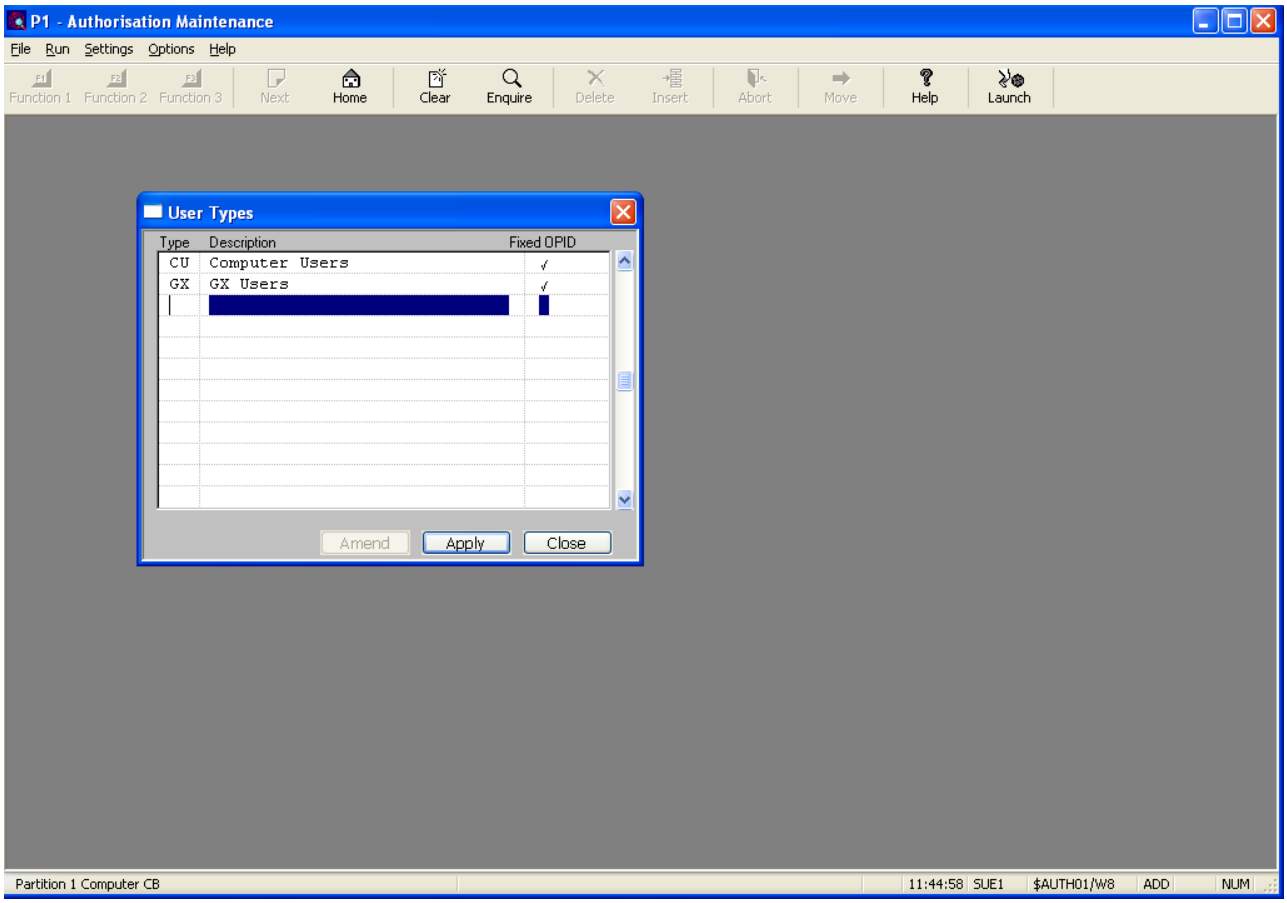
4.5 Clients

The ‘clients’ option from the main menu is for descriptive use only.

4.6 User Types

User types are for descriptive purposes only and are used to describe a user in the table of users.

Selecting the ‘User Types’ entry from the menu shows the current list of user types:

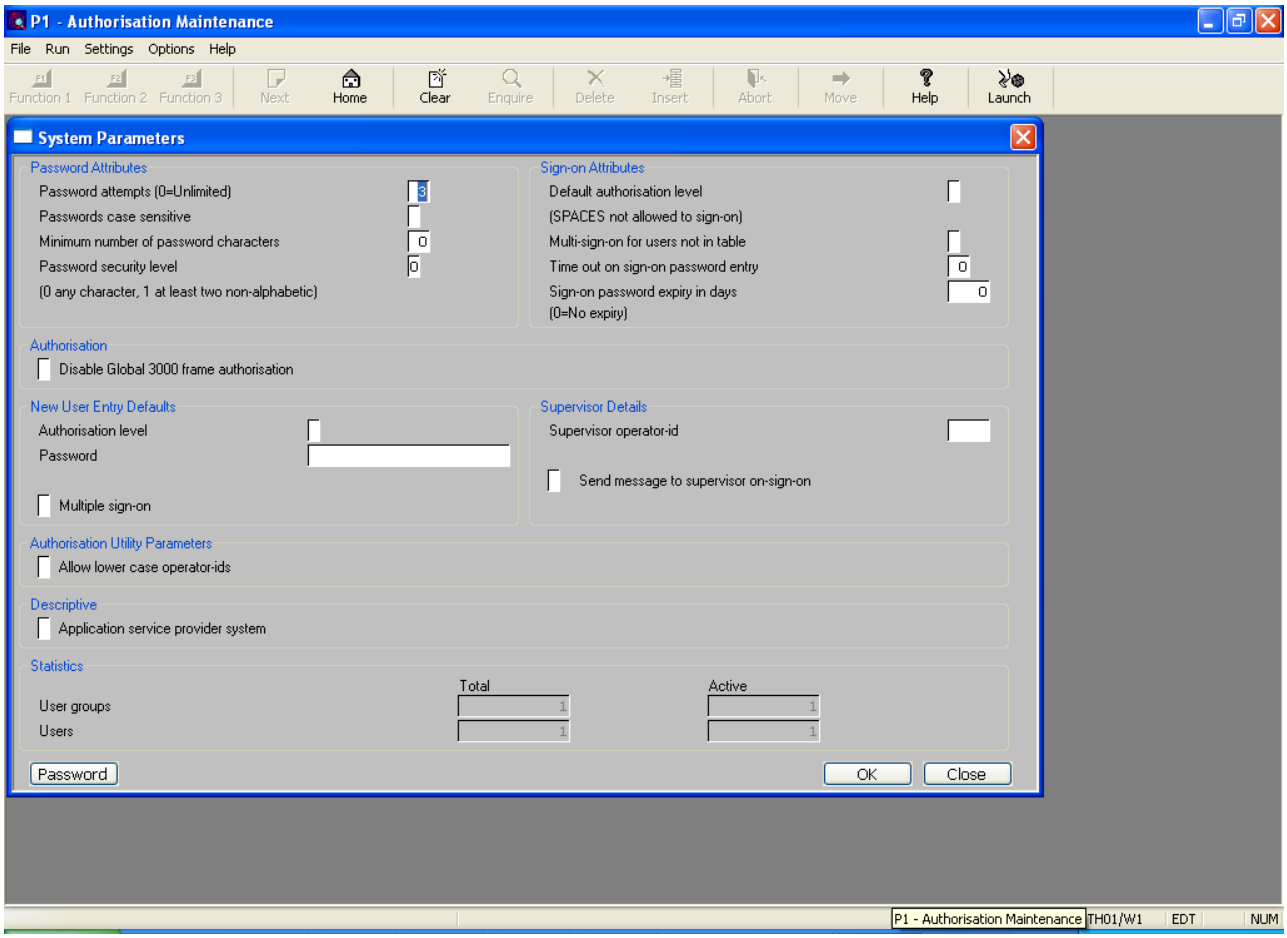


You may add a new user type to the end of the table. You may insert a new entry by pressing the 'Insert' button on the toolbar and you can delete an entry by positioning on that entry and pressing the 'Delete' button on the toolbar.

4.7 System Parameters

To amend the system parameters you must select the 'System Parameters' option from the main menu.

The current system parameter settings will be shown, which you may amend:



4.7.1 Password attempts

This is the number of attempts a user has to enter a password to gain access to either Global System Manager or to an authorisation point. A value of 0 indicates unlimited retries.

4.7.2 Passwords case sensitive

You may indicate if the validation of a password to access either Global System Manager or an authorisation point should be case sensitive.

4.7.3 Minimum of password characters

This is used to indicate the minimum length of a password. The maximum length of a password is 20.

4.7.4 Password security level

This is the level of security required for a password. There are currently only two options

0 - Any selection of characters may be used
1 - A password must contain at least two non-alphabetic characters

4.7.5 Default authorisation level

This is the authorisation level at which users who are not in the table of users will be signed on to Global System Manager. If the default authorisation level is set to spaces then users not in the table will not be allowed to sign-on.

4.7.6 Multi-sign on for users not in table

This is to indicate whether users not in the table are allowed to sign-on a multiple number of times. If this is set to SPACES then the default will be the value set in the System Manager customisation utility, $CUS. If it is set to any other value, and no override has been set using $CUS then this values will be honoured.

4.7.7 Time out on sign-on password entry

This indicates the time in seconds that Global System Manager will wait at the sign-on password prompt before automatically signing off again, If this time is set to zero then the System Manager password prompt will not time out.

4.7.8 Sign on expiry in days

This is the number of days for which a Global System Manager password is valid. If a user signs on after the password has expired a change of password will be forced. A value of 0 indicated that there is no password expiry time.

4.7.9 Disable Global 3000 Frame Authorisation

If this flag is set then the frame level Authorisation Points in Global 3000 applications will not be honoured. These are the authorisation points executed from the Global 3000 application menus.

4.7.10 New user entry defaults – authorisation level

This field is to make the addition of new operators to the table easier. It is the value that the authorisation field will be set to in the ‘user details’ window when a new user is added.

4.7.11 New user entry defaults – password

This option in available for GSM SP-24 and later. This field is the make the addition of new operators to the table easier. This is the value that will be set in the password field when a new user is added.

4.7.12 New user entry defaults – multiple sign-on

This field is to make the addition of new operators to the table easier. It is the value that the multiple sign-on flag will be set to in the ‘user details’ window when a new user is added

4.7.13 Supervisor Operator-id

This is the operator of the user delegated as the system supervisor.

4.7.14 Send message to supervisor on sign-on

If this flag is set the system supervisor will receive a message every time a user signs-on.

4.7.15 Allow lower case operator-ids

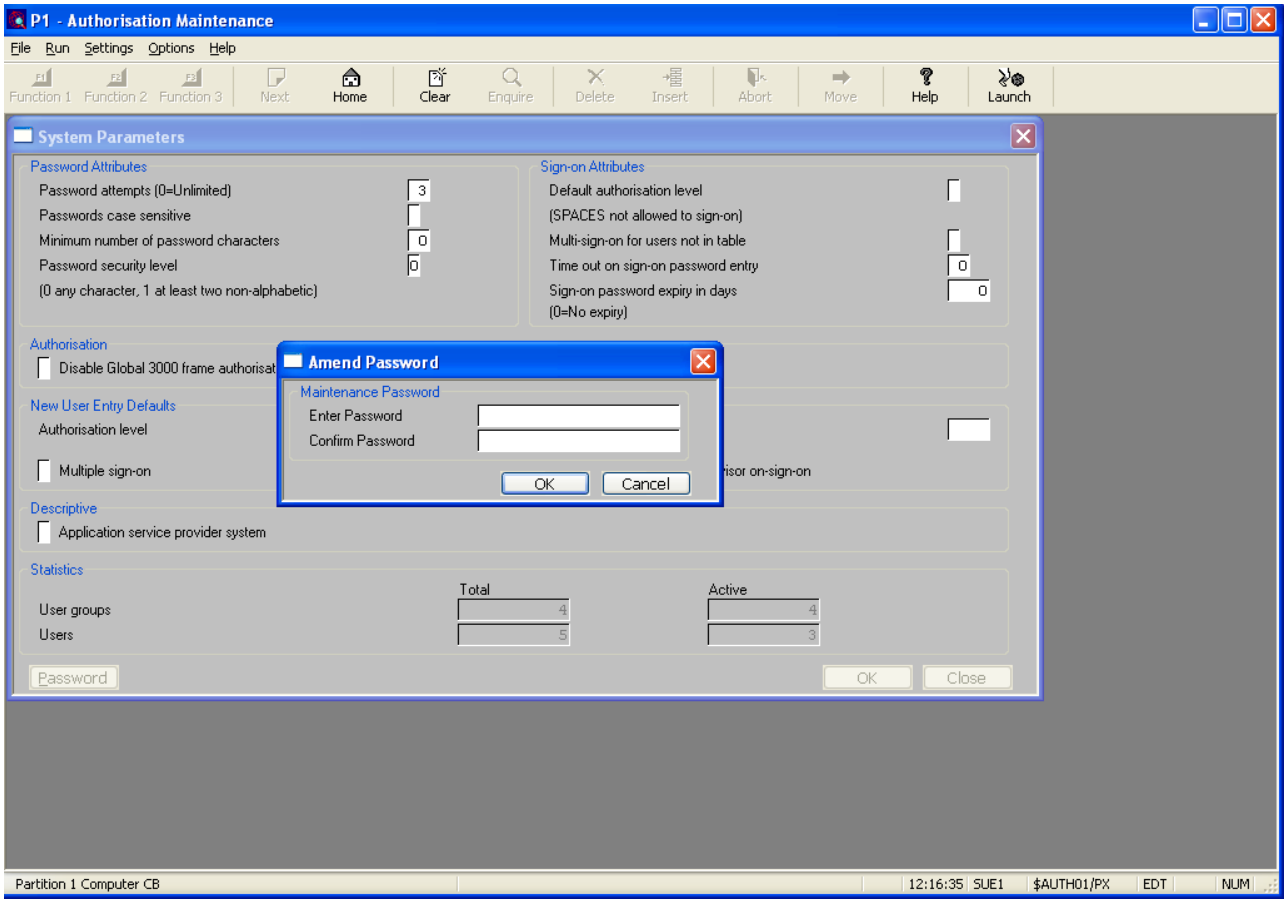
This option is available for SP-24 and later. Ticking this option allows you to key in a lower case operator-id for a user.

4.7.16 Application service provider

This flag is available for descriptive purposes only and indicates if this system is to be used as a service provider. If set it will allow the client list (see above) to be modified.

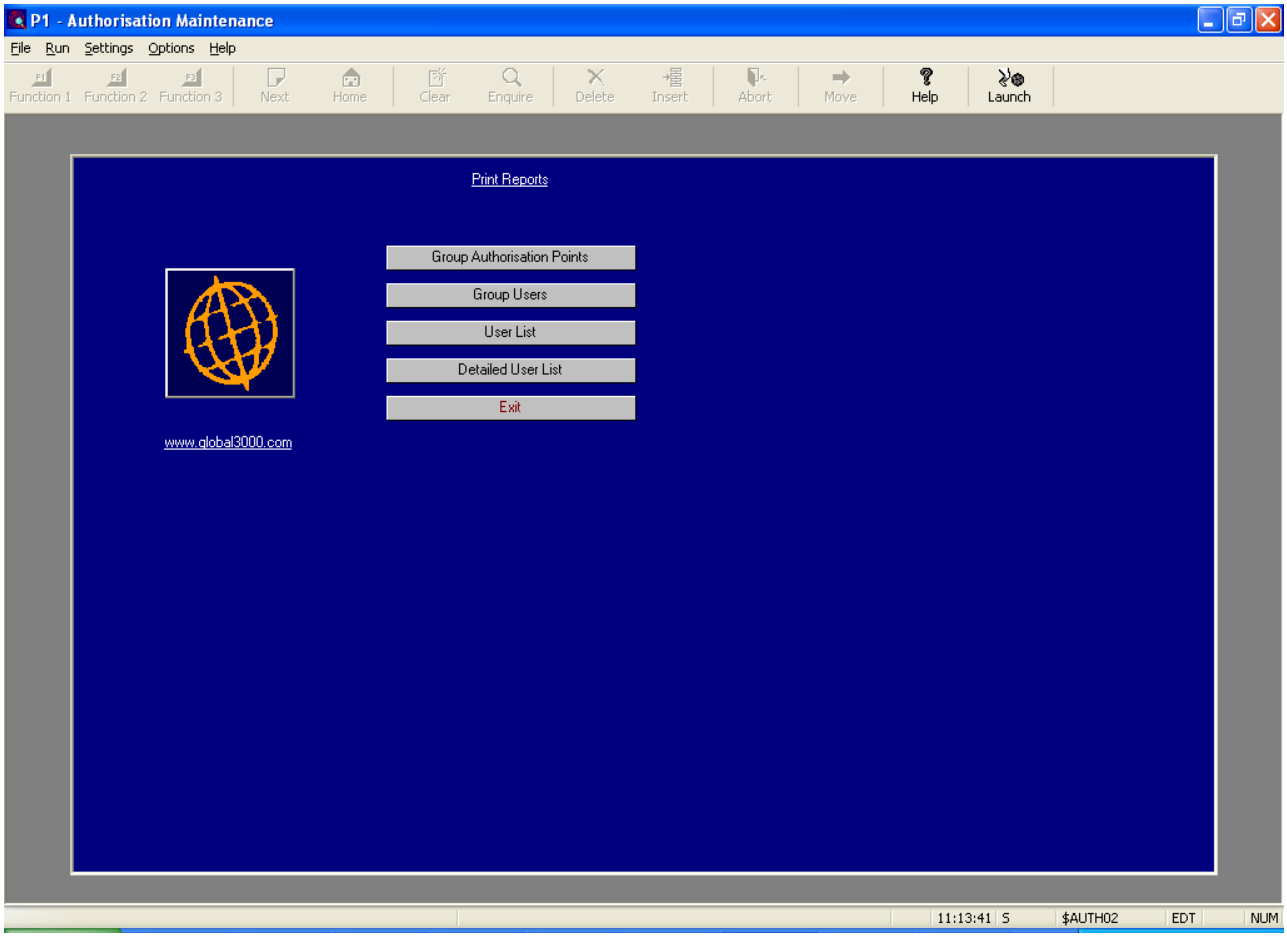
4.7.17 Password button

The password button allows you to set or amend the maintenance password required to run $AUTH32.



4.8 Print Reports

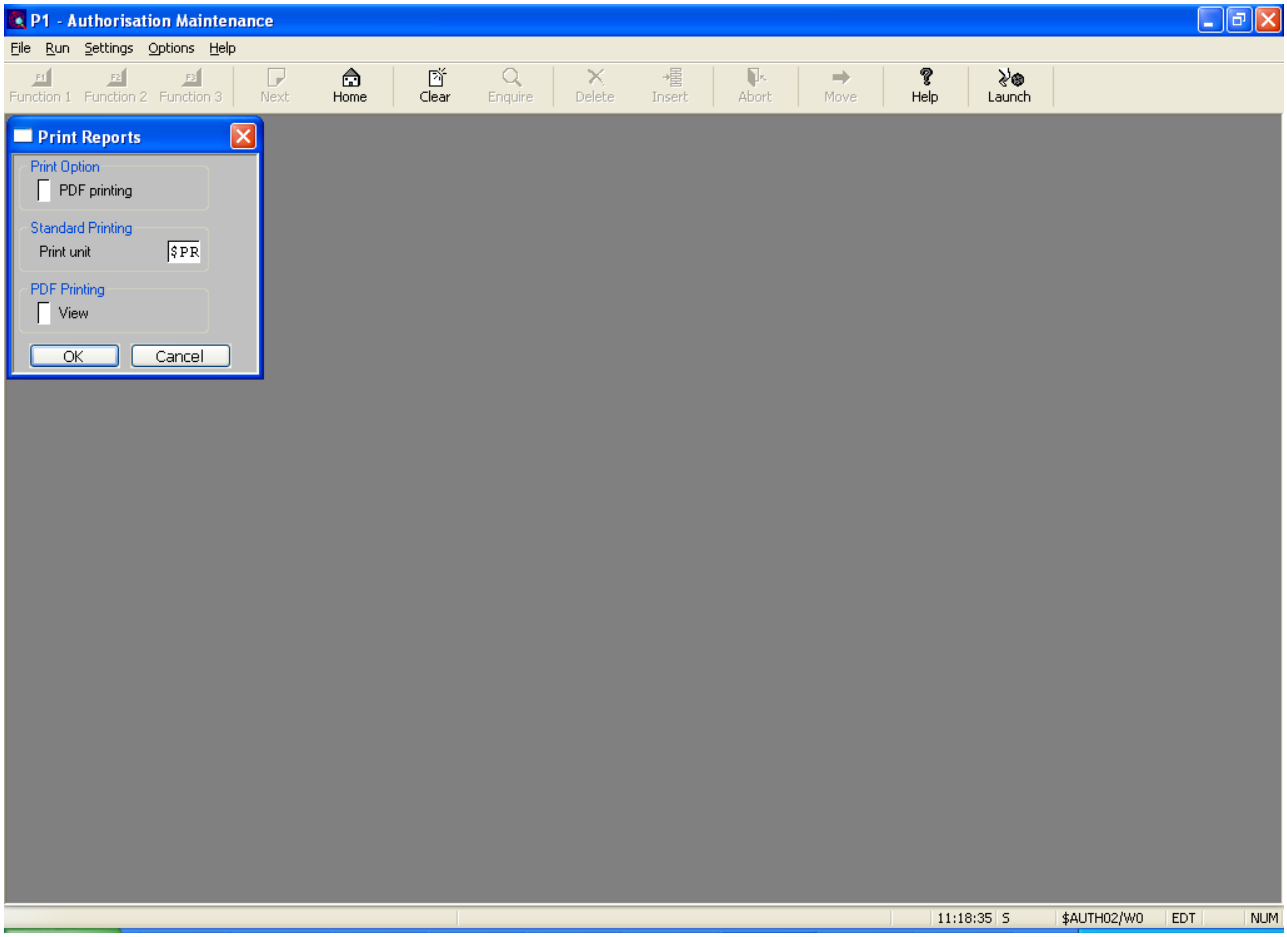
Selecting ‘Print Reports’ from the menu causes another menu to be shown, listing the print reports available.



4.8.1 Group Authorisation Points

The ‘group Authorisation Points’ entry lists the Authorisation Point overrides associated with all the groups.

When this option is chosen the ‘Print Reports’ window will appear as follows:



For systems before GSM SP-24 you may only key the output unit for the print report.

For GSM SP-24 and later you have the option to produce the report in PDF format. If you choose PDF format then you have the option of reviewing the report. If you do not chose PDF printing then you must specify the output unit for the print report.

4.8.2 Group Users

The 'Group users' entry prints all the users in the all the groups.

As above the 'Print Reports' window will appear to allow you to select the report output.

4.8.3 User List

This option only appears for GSM SP-24 or later.

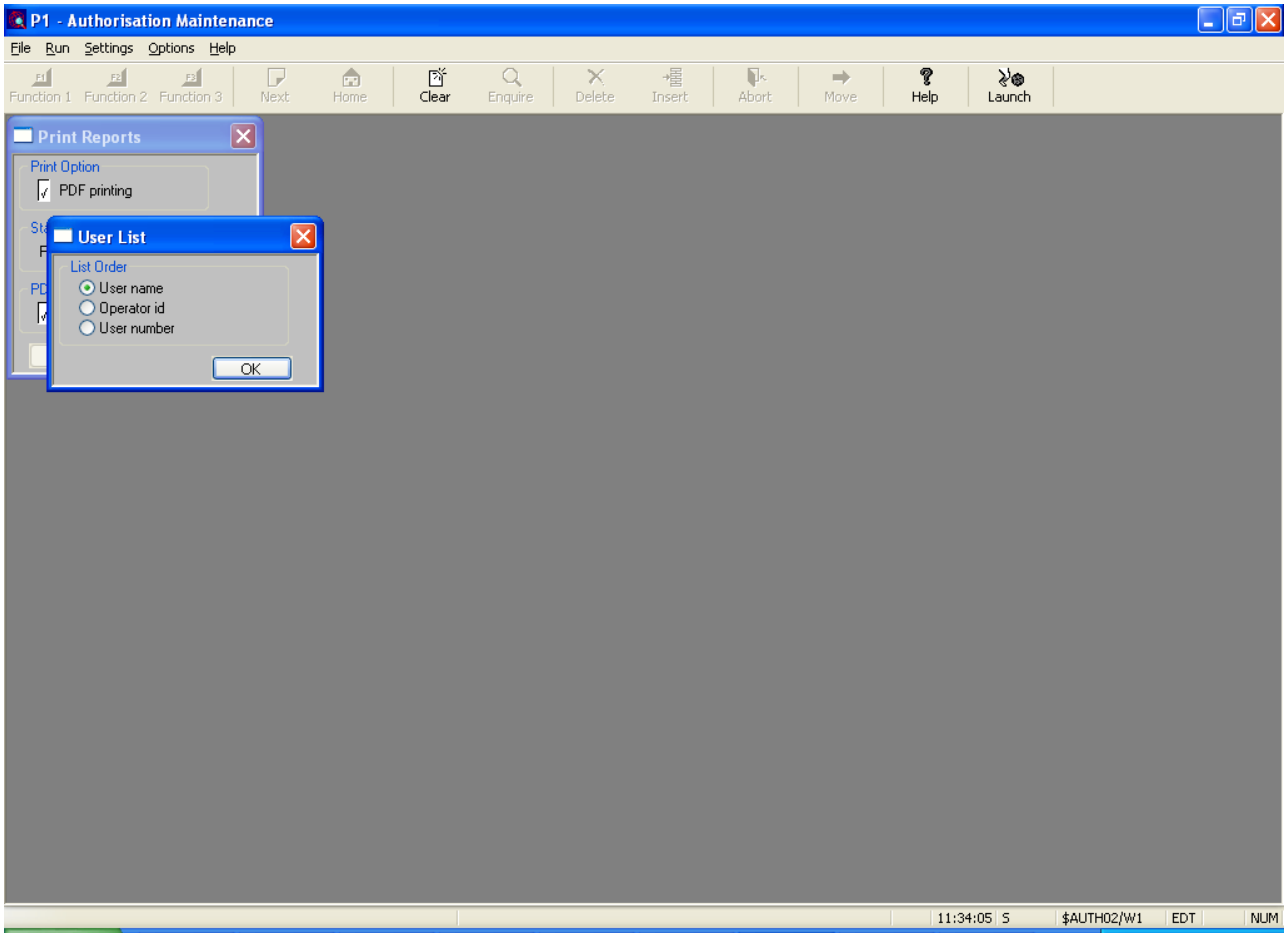
The 'User List' print prints the following details for all the users:

- User name
- User list reference number
- Operator-id
- Authorisation level

- Supervisor status
- Active status
-

On selecting this option the ‘Print Reports’ window will appear as above.

You can then choose the order in which the report should be printed:



When you have selected the order press the ‘OK’ button to continue.

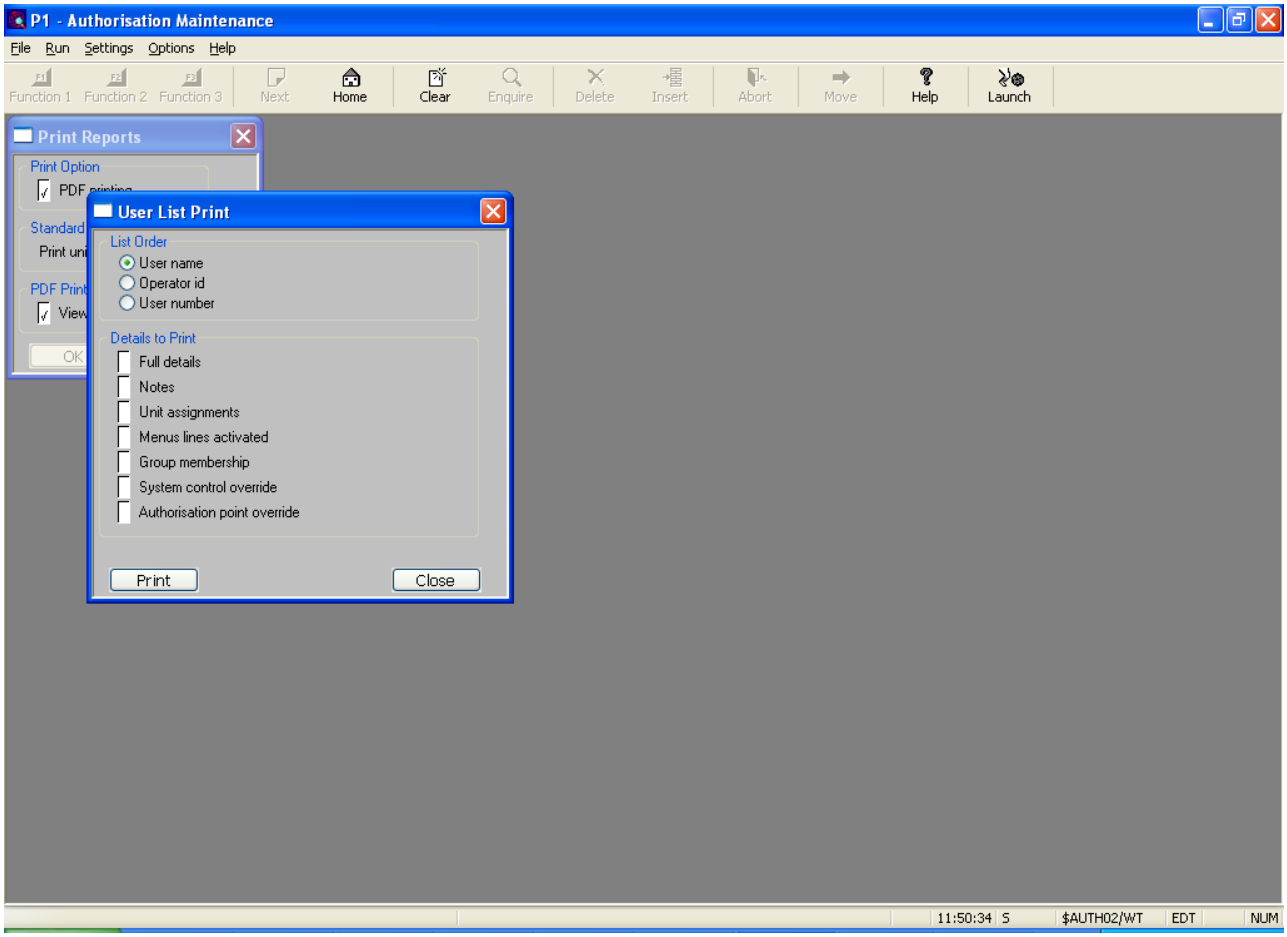
4.8.4 Detailed User List

This option only appears for GSM SP-24 or later.

This option allows the printing of selected details for the users on the system.

On selecting the ‘Detailed User List’ option the ‘Print Reports’ window will appear as above.

You will then be asked for the order in which you want the users to be printed and the details you want printed.



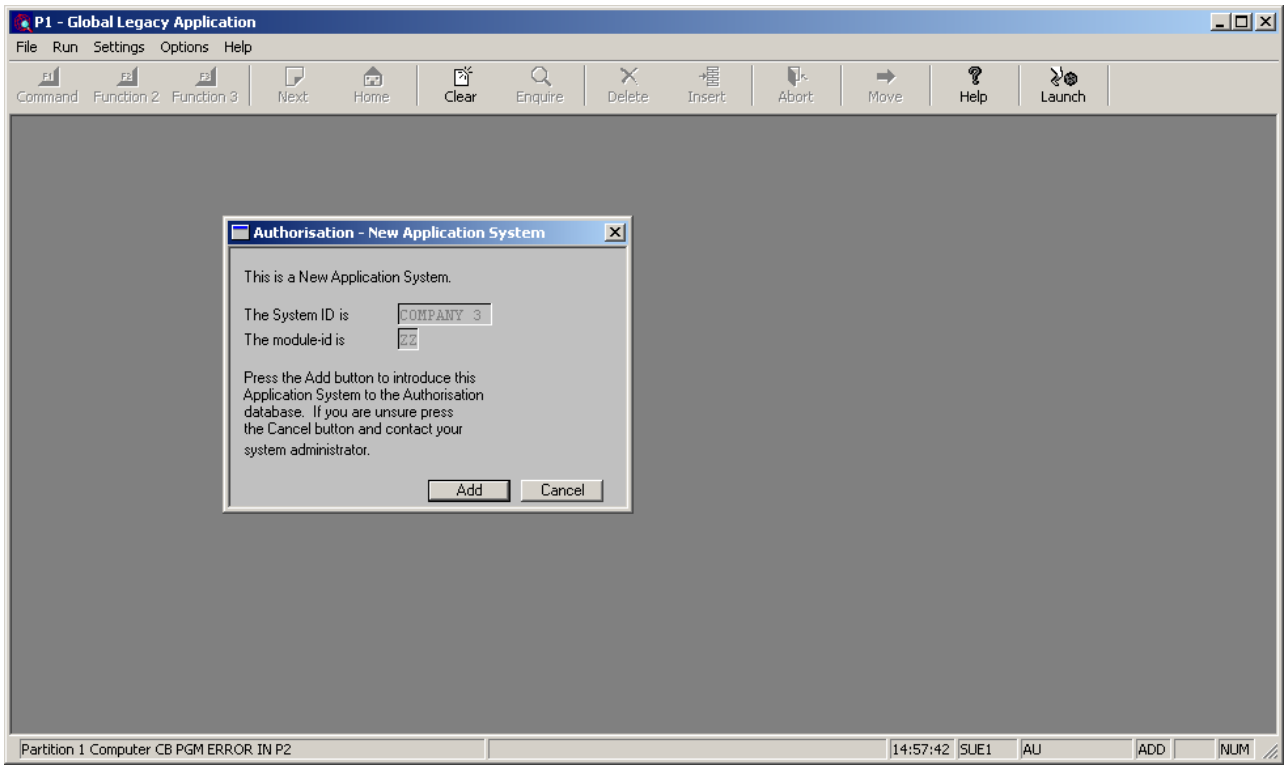
Once you have made your selections press the 'Print' button to print the report.

4.9 Exit

On exit $AUTH32 update the Global System Manager sign-on file. If this fails because there is insufficient space, you must increase the largest area available on the master SYSRES volume on unit $M.

5. Running an Application

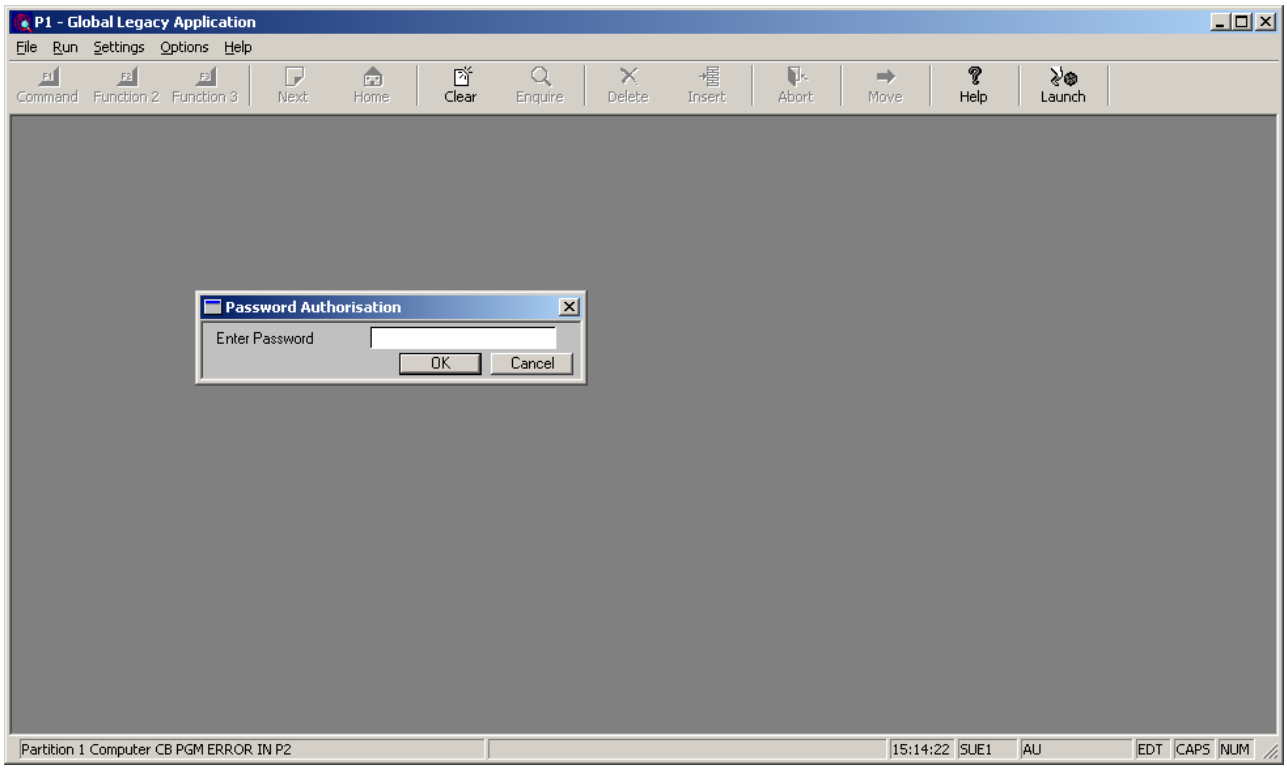
Provided the authorisation program in the $CUS 'Customise sign-on' function has been set to $AUTHEX, on first entering an application with a new system-id which has been entered in the authorisation database and where the authorisation points have not been loaded, you will be asked if you want to merge the Authorisation Points for this application.



Pressing the 'Add' button will add the Authorisation Points.

If you are not allowed access to any Authorisation Point in an application an appropriate message will be displayed and access will be denied. For example

If you need to enter a password to gain access to the Authorisation Point you will be asked for it.


P1 - Global Legacy Application
File Run Settings Options Help
Command Function 2 Function 3 Next Home Clear Enquire Delete Insert Abort Move Help Launch
Password Authorisation
Enter Password
OK
Cancel
Partition 1 Computer CB PGM ERROR IN P2
15:14:22 SUE1 AU EDT CAPS NUM