
Maintain Users and Groups

Prepared by:

Documentation Team

Prepared for:

Learning Resources

Module:

System

Date:

03 January 2017

Document Ref:

LMDSY0018

Version:

11.05

Construction Industry Solutions Ltd.
11 St. Laurence Way
SL1 2EA





Copyright 2016 Construction Industry Solutions Ltd.. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Construction Industry Solutions Ltd..

Construction Industry Solutions Ltd.
11 St. Laurence Way
SL1 2EA

THIS USER GUIDE WAS CREATED USING MADCAP FLARE.

Contents

1 How Function Security Works	1
2 Enquiring on function access	3
3 User Groups	4
3.1 Prime Groups	5
3.2 Main Groups and Subgroups	6
3.2.1 Setting Function Access Using Subgroups	8
3.3 Creating a Group	10
3.3.1 To set a group's function access using wildcards:	11
3.3.2 To set a group's access to specific functions:	11
3.4 Export Groups	13
3.5 Create a Group using the Import Functionality	14
4 Function Security	15
4.1 Recommended Approach	15
4.2 Parent and Child Functions	16
4.2.1 Generic Functions	16
4.3 Setting Function Security	17
4.3.1 Main Menu Security	18
4.3.1.1 Main Menu Security Exclusions	21
4.3.1.2 Main Menu Security Exclusions Example	22
4.3.2 Add Functions to Menu Headings using Interactive Security Update	25
4.3.2.1 To Remove Interactive Mode	27
4.3.3 Find Functions	28
4.3.4 Deny Access to Individuals	30
4.3.5 Hide Tabs	32
4.3.6 Access to Fields	33
4.3.6.1 Hiding Fields Across All Screens	33
4.3.6.2 Group Field Access	34
4.3.6.3 Hiding Fields in One Screen Only	35
4.4 Set Menu Security Utility - Overview	36
4.4.1 Business Reasons for Change	36
4.4.2 Initial Setup	36
4.4.3 Set Menu Security - Screen and Processing Changes	37
4.4.3.1 Report Mode	37
4.4.3.2 Update Mode	38
4.4.3.3 Undo Mode	38
5 Set Up a User	40
5.1 Details Tab	42
5.2 Groups Tab	46
5.2.1 Groups	46
5.2.2 Roles	46
5.3 Printing Tab	48
5.4 Coinsplus Tab	49
5.5 Preferences Tab	50
5.6 Wiki Tab	62



6 Removing a User	63
6.1 To disable a user in a secure manner:	64
7 Run a User Report	65
8 User Views	66
9 Creating Buyers	69
9.1 Main Tab	70
9.2 Contacts Tab	71
9.3 Personal Tab	72
10 Contract Security	73
10.1 Configuration	74
10.1.1 JC/JOBSEC	74
10.1.2 JC/COSECDEF	74
10.2 Application	75
10.2.1 Setting Contract Security by Code	76



1 How Function Security Works

When a user attempts to access a function:

- COINS checks the access permissions for the user (as set up in User Function Access). If the user has explicitly been allowed or denied access, this overrides any group permissions that may have been set up.
- If you are using Menu Item Security, COINS checks the parent function, which is an item on the COINS menu, to see whether the user has access and the function is of the correct access type.
- If the user has access to the parent, they have access to the child function by default, unless the permission has been explicitly overridden.

If the function is a menu, container or tab function, and the user has access to a function on that menu, container or tab, then the menu, container or tab is available.

- If the user's permission is G-Group access (the default), COINS checks the permissions for each group that the user belongs to, in the order the groups are defined on the user record, beginning with the Prime Group.
 - a. COINS checks the can-do lists of functions and role types that are allowed or denied on the group. If the function is included in any of these lists, the user is allowed or denied access accordingly. (Within the same group, deny takes priority over allow.)
 - b. COINS then looks at the permissions for specific functions set up on the group record. If the group is allowed or denied access then that is the result.
 - c. If you are using Menu Item Security, COINS then checks the group access for the parent function; if the group is allowed access to the parent and the access type of the parent is the correct type, then the user is allowed access.
 - d. If the group record indicates G-Group access, COINS checks the next group.



Because COINS evaluates the permissions on each group in turn, the sequence of the groups on a user's record is important. If a group denies access to a function, the user will not be able to access the function, even if a later group would allow access.

- Finally, if you have role-based licensing and your licence includes roles that are appropriate, you can use these to grant access to users. If the user is not a "named role" user COINS checks any roles assigned to the user:
 - a. If the function is included in the "Allow" can-do lists of functions or role types on any of the roles, the user is allowed access unless explicitly denied by user or group access permissions.
 - b. If the function is denied by the role, COINS continues by checking the user and group permissions. The user may still have access if allowed by user or group access permissions.



If the user is a "named role" user, they will **ONLY** be able to access functions allowed by their roles; see Role-Based Licensing.

If none of the groups or roles explicitly allows access then the user is not allowed access.



When you create a new user record, all the permissions for that user are set to G-Group, so they only have access to those procedures and menus permitted for their group, until you explicitly change their access permission. Similarly, when you create a new group, all the permissions are G-Group. This means that, if you were to create a new group, and assign users to that group, without explicitly granting access permissions for either the group or the users, the users in that group would not be allowed access to anything.

COINS always has a user called "SYSAdmin" and a group called "root". The SYSAdmin user has permission to do anything, as does any user who is in the root group who is not explicitly denied access.

The following illustration shows how group access permissions affect the access of individual users. For a particular function, group A allows access, group B denies access, and group C specifies group access:

	User Function Access	First Group	Second Group	Role	Does the user have access?
User 1	N	Group A (Y)	Group C (G)		No
User 2	G	Group A (Y)	Group B (N)		Yes
User 3	G	Group B (N)	Group A (Y)		No
User 4	G	Group C (G)			No
User 5	G	Group C (G)		Role R (Y)	Yes



If you are using Menu Item Security:

If a function is a menu, the user may be allowed access because they have been given access to a menu item on that menu.

If the function is a child, the user may be allowed access because they have been given access to the parent function



2 Enquiring on function access

You can enquire on what access a user has to a function:

- In System > User Maintenance > Users, click the link in the User ID column.
- Click the User Function Access tab.
- Filter on the function you want to enquire about.

The Allowed column is ticked if the user has access to the function. The Access, Group and Role columns show whether the access or denial comes from the user function permissions, from a group, or from a role.



3 User Groups

You can set permissions for several users together using groups. Each user belongs to one or more groups. Each group specifies the functions that members of the group have access to (and may also specify functions that members of the group are denied access to).

You can define the permissions on a group by building them up from the permissions on other groups. This means you can create sub groups that give access to related functions, and list the appropriate sub groups on each "main" group. See Main Groups and Subgroups.

You can specify groups of functions, using wildcards, to provide a "broad brush" set of access permissions; you can then "fine tune" this by specifying additional functions to which the group has or does not have access.

For example:

You might set up a group for people using Purchase Ledger, allowing them access to all except the Maintenance, Administration and Set-up options. Everyone who belongs to this group would, by default, be able to access these options. You might have one user in the group who only needs to use the enquiries options, so you would restrict the individual access for that user. You might also have a supervisor, who needs access to the Maintenance, Administration and Set-up options, so you could extend the individual access for that user. How to do this is explained in Menus.



3.1 Prime Groups

Each user is assigned to a prime group. In conjunction with the user's security level, this controls whether the user has access to reports and batches created by other users. You have access to another user's reports and batches if:

- That user's prime group is included in your group list, and
- Your security level is higher than the other user's security level (or the security levels are equal, if the SY parameter EQUACCESS is set to Y).

Because of this, we recommend that you have separate groups for data access (batches and reports) and for function access.

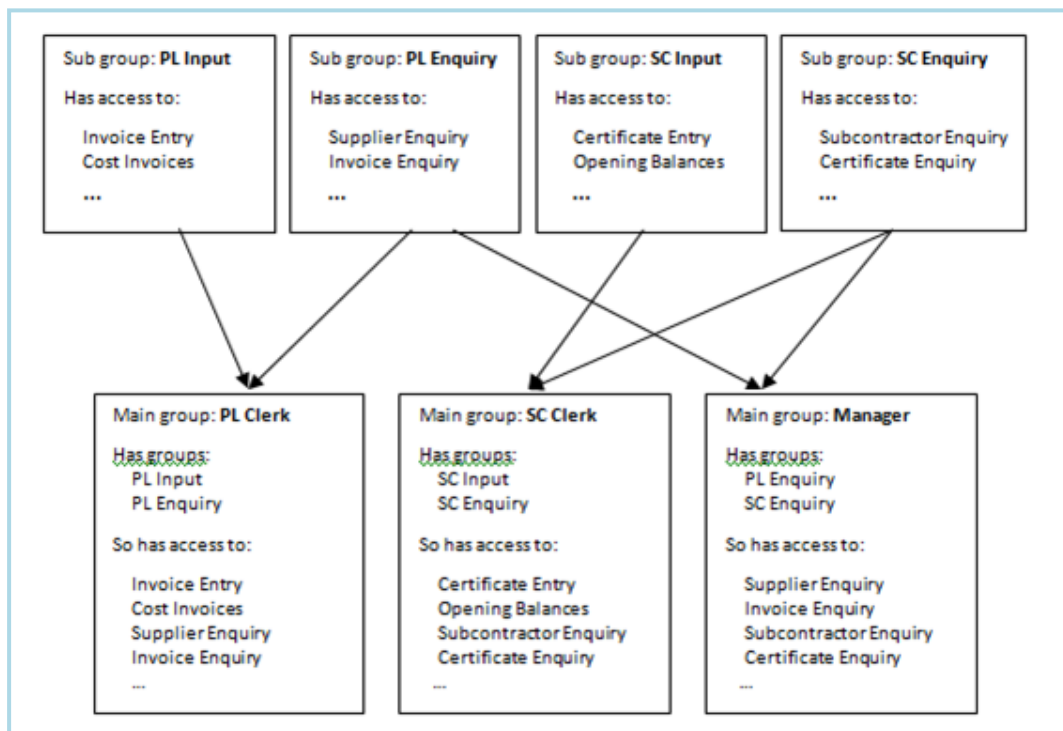
3.2 Main Groups and Subgroups

It is possible to assign the group access permissions by reference to other groups. A field on System > User Maintenance > Groups allows you to list subgroups for the group. This means you can create "building blocks" of access permissions (at the subgroup level), that can be combined to create an "access profile" for a main group. This effectively allows you to set up a main group as a job role or "model user". You then assign each user to a main group. The content of the role is independent of the users assigned to it and you can change it without mass changes to the users.



It is possible to assign users to more than one group. However the intention if using the main group/subgroup approach is to have a separate group for each job role. This may be more appropriate for large organisations with clearly defined job roles.

For example you might create a main group PL Clerk that is assigned access from two subgroups: PL Input and PL Enquiry. You can set the access permissions for the PL Clerk group by setting the access permissions for PL Input and PL Enquiry and setting the PL Clerk group to inherit access from these two subgroups.



When you have set up the subgroups, you need to run a process to set the access on the main group. This process evaluates the subgroups in turn (much like the group access is evaluated on a user); as soon as a Y-Allow or N-Deny is found in the subgroups assigned, the Y or N is set on the main group being evaluated. This is equivalent to compiling the subgroup access to create the main group access. (You could then modify the main group but we do not recommend this since, if you were to re-run the process, the main group access would again be overwritten by the evaluated subgroup access.)



If you change the permissions on a subgroup or change the list of subgroups on the main group, the changes will not apply to the main group until you re-run the process.

You can then assign user access by setting the groups on the user. Either main groups or sub groups can be used for this.

If a sub group access is changed, the main group access can be re processed; you do not need to modify the main groups themselves.

COINS only evaluates one level of sub groups during the process; it is not recursive down to further levels of sub group. (If you choose to build a set of groups from a set of sub groups you could then use the evaluated groups as sub groups to further groups by processing them in order.)



3.2.1 Setting Function Access Using Subgroups

Group access permissions can be built up from subgroups, and the permissions are then copied to the groups. This means you can set up groups that correspond to job positions or roles, using subgroups to dictate the access permissions for collections of related menu items. When a new member of staff joins, you can easily set up their access permissions by setting up one group on their user record. It also has the advantage that you can modify the permissions while users are using the system, without affecting their access, and then apply all the changes together at a suitable time.

We recommend the following:

1. Set up sub groups to collect together the functions that relate to the business processes each job position requires. In particular, set up separate groups for input and enquiry. We recommend you set up subgroups for related functions and types of access. For example:
 - A subgroup for PL Enquiries and Reports (with read-only access).
 - A subgroup for PL Invoice and Payment Entry (with update access).
 - A subgroup for PL Administration and Maintenance functions (with update access).
 - Use System > User Maintenance > Groups to create subgroups.
2. Specify the access permissions to collections of functions.
 - To set the access permissions, you can use:
 - System > User Maintenance > Function Security > Main Menu Security, entering the code for the subgroup.
 - The Group Function Access tab while maintaining the subgroup in System > User Maintenance > Groups.
3. Set up main groups that correspond to roles or job positions in your organisation.
 - Do not set up any access permissions on the main groups. If you introduce a new position with different responsibilities, set up a new group.
 - We recommend you set up main groups to correspond to user roles or job titles, and that you do not set up access permissions on the main groups; use sub groups for setting access permissions. This is because if you change the permissions on a main group, these will be overwritten when you next process the sub groups -- the first thing the process does is to delete all existing group permissions.
 - Use System > User Maintenance > Groups to create main groups.
4. Add the appropriate subgroups to each group.
 - Assign one or more sub groups to each main group, according to the features you want that main group to have access to. Use the multiple selection Sub Group field to select the sub groups from the list.
 - The order of the sub groups is important; when the sub group



permissions are processed, COINS will go through each sub group in turn and apply any explicit access settings (Allow or Deny) from the sub group to the main group. It will then only apply explicit access settings from the next sub group if they have not been set by the previous sub group. So if you allow access to a function on the first sub group, and deny access on the second sub group, the main group will allow access.

- In practice we do not expect Deny access to be used very often. However if you are using Menu Item Security, the order in which Read-Only access and Update access are specified may be important.

5. Use Sub Group Process to set the access permissions on each main group based on the sub groups that belong to it. Processing the access permissions on groups involves running a function that evaluates the permissions on each sub group assigned to a group, in turn, and copies the permissions to the main group. This means that you can change the access on sub groups, and then only need to reprocess the main groups.

- Go to System > User Maintenance > Sub Group Process.
- Specify the groups you want to process.

As well as copying the function access permissions to the main groups, this also copies group field security and HS sales event security settings from the sub groups to the main groups.

6. Assign each user to one or more main groups.

- Use System > User Maintenance > Users to specify the group or groups each user belongs to.
- Go to System > User Maintenance > Users.
- Click OPEN to open a user record.
- NOTE: Because COINS evaluates the permissions on each group in turn, the sequence of the groups on a user's record is important. If a group denies access to a function, the user will not be able to access the function, even if a later group would allow access.
- On the Groups tab, select the main group that corresponds to the user's job position.
- Click SAVE.

7. If necessary, fine-tune the access for individual users; you can use any of the function security features to do this.



3.3 Creating a Group

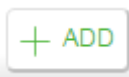
From the System menu, select User Maintenance and then Groups.

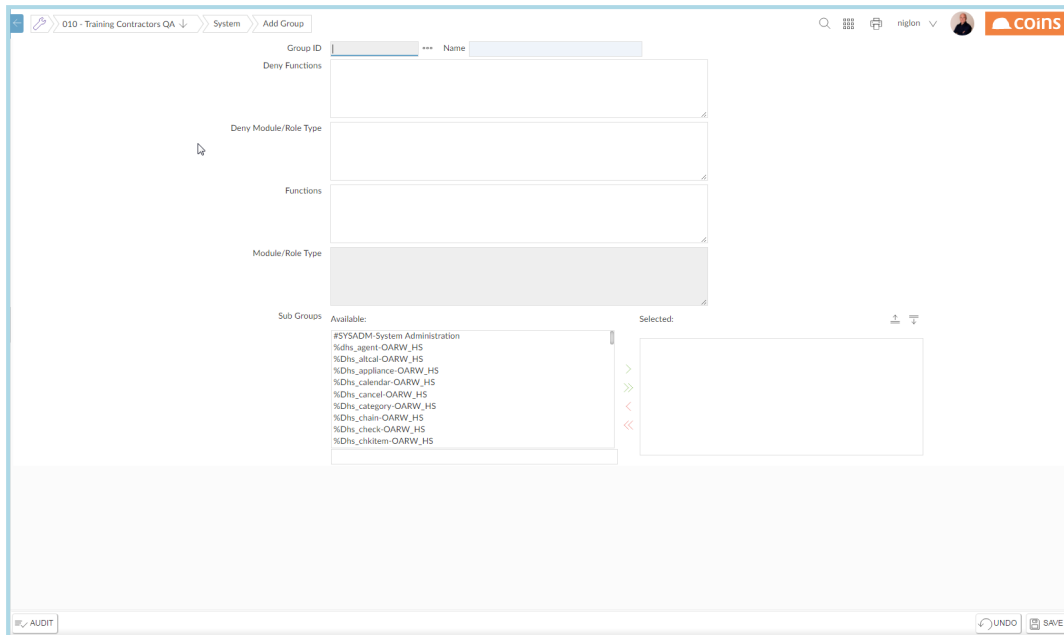
Group ID	Name
FBUpdPL	Firstbase Update-Purchase Ledger
FBUpdPO	Firstbase Update-Procurement
FBUpdPR	Firstbase Update-Payroll
FBUpdPT	Firstbase Update-Project Management
FBUpdSC	Firstbase Update-Subcontract Ledger
FBUpdSL	Firstbase Update-Sales Ledger
FBUpdSRM	Firstbase Update-Supplier Relationship Management
FBUpdSS	Firstbase Update-Health & Safety
FBUpdST	Firstbase Update-Stock
FBUpdSV	Firstbase Update-Commercial Manager
FBUpdSY	Firstbase Update-System
FBUpdSYD	Firstbase Update-Documents Management
FBUpdSYN	Firstbase Update-Release Notes
FBUpdSYR	Firstbase Update-OA Reporting & BI
FBUpdVA	Firstbase Update-Valuations
FBUpdVP	Firstbase Update-VAP
GLINPUT	OA GL Input
GLINPOA	OA General Ledger Input Only
GLINPUT	OA GL Input
groupstest	test group



In the Group ID column you will see a list of groups beginning with #. These groups are for Coins+ and cannot be used in OA because OA uses different functions from Coinsplus. Coins+ users need to use the #menus to allow the use of the F6 switch to toggle between users and groups. #menus are not relevant to customers who use OA only.

Click



Enter a name and description for the group.

3.3.1 To set a group's function access using wildcards:

- Go to System > User Maintenance > Groups.
- Click OPEN to open the group record.
- In the Deny Functions and Functions fields, enter can-do lists for the functions you want to deny or allow access to.
- For example, if you want to allow access to all the functions in Purchase Ledger except the supplier update functions, you could set up a group with %WPL* in the Functions field, and %WPL2000BAVMA,%WPL2000BAVMU,%WPL2000BAVMD in the Deny Functions field. This would deny the ability to add, update or delete a supplier.
- Alternatively, to allow some users access to all the functions in Purchase Ledger, you could set up two groups, an "allow" group which gives access to %WPL*, and a "deny" group which denies access to the add, update and delete supplier functions. If you put this "deny" group before the "allow" group in a user's group list, that user will not have access to the add, update and delete functions; other users without the "deny" group but with the "allow" group will have access to all the Purchase Ledger functions.
- If there are roles that provide the functions you want, you can add these to the group; users who belong to the group will have access to all the functions in the role (or will be denied access, if you enter the role in the Deny Module/Role Type field).
- Click SAVE.

3.3.2 To set a group's access to specific functions:

These only take effect if the functions are not already included in the "allow" or "deny" lists - see above.

- Go to System > User Maintenance > Groups.
- Click the link in the Group ID column of the group whose access permissions you want to change. COINS displays the Group Function Access screen for that group.



You cannot change the access rights for the Root group or SYSAdmin user.

- Select the record or records you want to set permissions for.
- In the Choose Action list, select:
 - Set Access to Yes-Update to allow update access (only available if you are using Menu Item Security)
 - Set Access to No to prevent access.
 - Set Access to Group to use the setting from the next group in the user's list.
 - Set Access to Yes to allow access (or to allow read only access if using Menu Item Security)

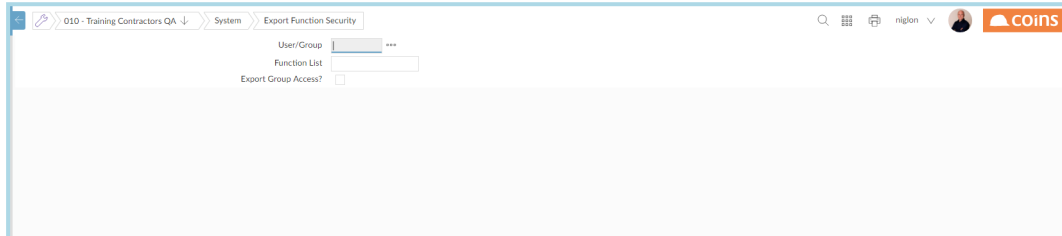


Because COINS evaluates the permissions on each group in turn, the sequence of the groups on a user's record is important. If a group denies access to a function, the user will not be able to access the function, even if a later group would allow access.

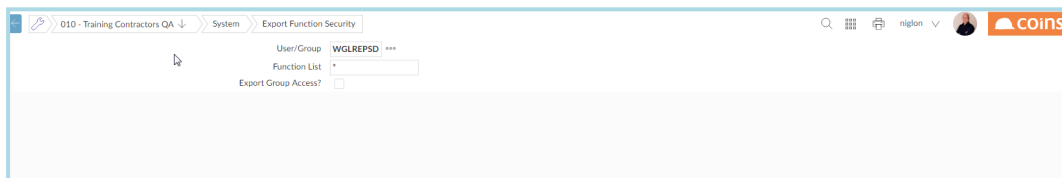
3.4 Export Groups

You may want to export a group to Excel, for instance if you have created a Group in COL you could then export it into Live.

- From the System Menu, select **User Maintenance > Function Security > Export Function Security**



- Select the group you want to export from the lookup and enter an asterisk in the Function List field.



- For Export Function Access, the options are:

- Blank = All functions will be exported.
- Ticked = Only functions which have been explicitly set to either access Yes or No will be exported.

- Click  the following screen will be displayed:



- Press Ctrl A in the Function Security Data screen to highlight the contents field,
- Press CTRL-C to copy to the clipboard
- You can now open Excel and paste the contents

3.5 Create a Group using the Import Functionality

Groups exported from one environment, using the 3.4 , Export Groups function, can be imported into another environment using the Import Function Security option.

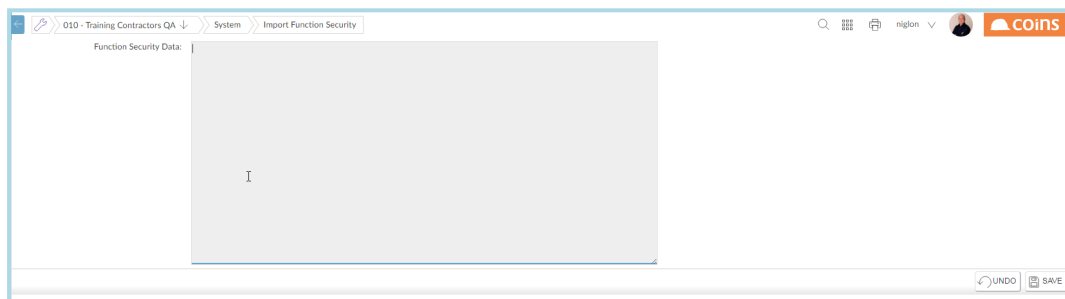
- Create a Group



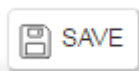
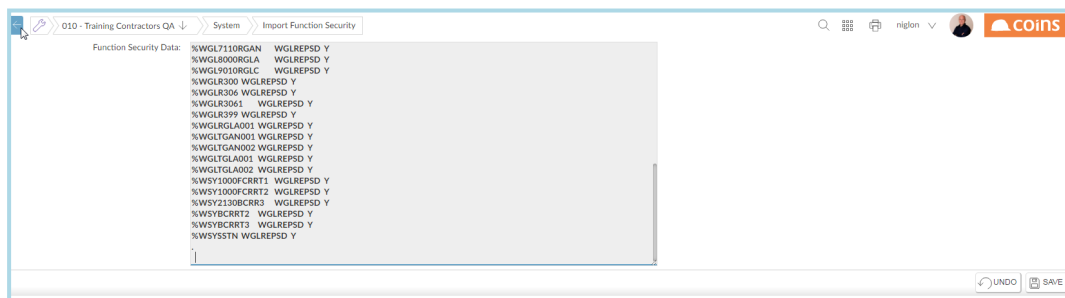
The Group ID you create in Group Maintenance must be the same name as that in the import file. For instance, if the file is for a group called WMANDATORY the group ID you create in Group Maintenance should be WMANDATORY.

- From the System Menu, select User Maintenance > Function Security > Import Function Security

The following screen will be displayed.



- Open the file created from the Export; use Ctrl-A to select all the contents (including the last line with the period symbol)
- Paste the contents into the Function Security Data screen



- Click
- A blank Function Security Data screen will be displayed; Click Undo.
- The group can now be assigned to users.



4 Function Security

Function security relates to the level of access that users have to COINS functions. A function in COINS OA can be: a menu, a menu item, a tab, an option or action item, and so on. Also, many of the features that allow you to update information on a screen - such as buttons - also have associated functions that can be used to control access.

Each function can be made secure so that only users of appropriate authority are able to access it. If a user is not permitted to run a particular function then it will not appear on their screen. So for example:

- If a user does not have access to a menu item, it will not appear on their menu.
- You can prevent a user from updating records on a screen by denying them access to the update function associated with that screen.

There are various ways to maintain user access permissions:

- You can set permissions for groups. Users inherit the permissions of the group (or groups) they belong to.
- You can build up permissions for groups from permissions that are specified on sub groups.
- At both group and sub group level, you can grant or deny access to functions by using wildcards; this provides a "broad brush" control over which functions are available. You can also specify access to individual functions.
- You can set permissions for users; these override the permissions the user inherits from the group.
- If you use Menu Item Security, you can grant read-only or update access, or deny access, at the level of menu items; COINS automatically determines the appropriate permissions for any functions or other options within the menu item. You can do this for users, groups or sub groups.

You can also control access to individual fields; see Access to Fields.

4.1 Recommended Approach

We recommend that you:

- Set up main groups that correspond to the job positions in your organisation. Do not set up any access permissions on the main groups. If you introduce a new position with different responsibilities, set up a new group.
- Set up sub groups to group together the functions that relate to the business processes each job position requires. In particular, set up separate groups for input and enquiry.
- If you have Menu Item Security enabled, Use System > User Maintenance > Function Security > Main Menu Security to set up access permissions on each sub group that provide access to the menu items required for the process.
- Use the other function security options (roles, group security maintenance, Interactive Security Maintenance) to fine tune the access permissions for the sub groups.
- Add the sub groups to the appropriate groups and process each group to copy the access permissions from the sub groups.
- For each user, assign one main group according to their job position.



4.2 Parent and Child Functions

The vast majority of functions are subordinate functions to a menu item. For example the payments tab on the supplier maintenance screen is subordinate to the supplier maintenance screen which is itself subordinate to the supplier browse that appears on the menu. Each function in the system is assigned a parent function that resides on a menu. Functions that reside on a menu have themselves as parents, and are referred to as "menu items".

If you are using Menu Item Security, COINS looks at the parent function when determining whether to grant a user access to a function; if the user has access to the parent, COINS automatically grants access to the child (unless this has been specifically denied using detailed function security).

Even if you are not using Menu Item Security, you can use System > User Maintenance > Function Security > Main Menu Security to see the children of a function.

4.2.1 Generic Functions

Some functions do not belong to an individual parent but are used on several different functions (sometimes across several modules); for example: Post Batches, Post Batches with Report and Batch Posting/Listing Report. These functions have been placed on special menus in each module which have codes of the form %WxxCO, where xx is the module code and CO indicates "common" -- the functions on the menu are common to the module (for example: %WPLCO). The default for functions like this will be no access; you can set access permissions for these in exactly the same way as 'normal' functions. The special menus are never displayed in the menu tree, but are shown at the end of the module menu in the function access maintenance screens. This helps you decide which generic functions you need to consider for a module.

Some functions are generic functions which users should have access to in order to use COINS properly (for example, the Batch Details Tab and Batch Transactions Tab on the batch summary, which apply to all batches of all batch types). These functions do not belong to a specific menu item, but are fundamental to the use of COINS. This type of generic function has a role type of SYS. If you are using Menu Item Security, any function with the role type SYS is available to all users. You can deny access to functions like this if you really think it is necessary, but this is not the intention.



4.3 Setting Function Security

There are various ways to set up access permissions for specific functions:

- **System > User Maintenance > Function Security > Main Menu Security** allows you to apply function security for a user or group. This presents you with a list of the functions on a module, in the order in which they appear on the menu.
- User Function Access is part of **System > User Maintenance > Users** and allows you to set an individual user's permissions for all functions. Group Function Access is the equivalent method in **System > User Maintenance > Groups**.
- **System > User Maintenance > Function Security > Interactive Security Update** allows you to control what access a user or group has to functions and subfunctions (such as buttons).
- When you select the user or group you want to grant security for, COINS opens a second window in which you can go to the page for which you want to set the permissions, and a third window in which you can set the access that the user or group has to the various functions on that screen.
- Within **OA Reporting & BI > Functions > Function Maintenance**, when you update a function, the Function Security by User tab lists the users and groups, and allows you to maintain whether they have access to this function. If the function has sub functions (Add, Update, Delete, Export, Bulk) you can also maintain whether the user or group has access to each of these. The multi-update button MULTI allows you to set the access for multiple users/groups in a single update.

4.3.1 Main Menu Security

If you are creating groups from scratch, you will need to give access to the required menu headings and the functions for the groups. It doesn't matter which order this is done i.e. you can use interactive security update to give access to the functions and then give access to the headings.

Main Menu Security allows you to apply function security for a user or group. This presents you with a list of the functions on a module, in the order in which they appear on the menu.

If you are using Menu Item Security you can set the access permissions at the level of menu items; the child functions inherit the permissions from the menu item.

If you are not using Menu Item Security, you can set the access permissions for the menu items, and follow a link to a screen that lets you set the permissions for the child functions of each menu item.

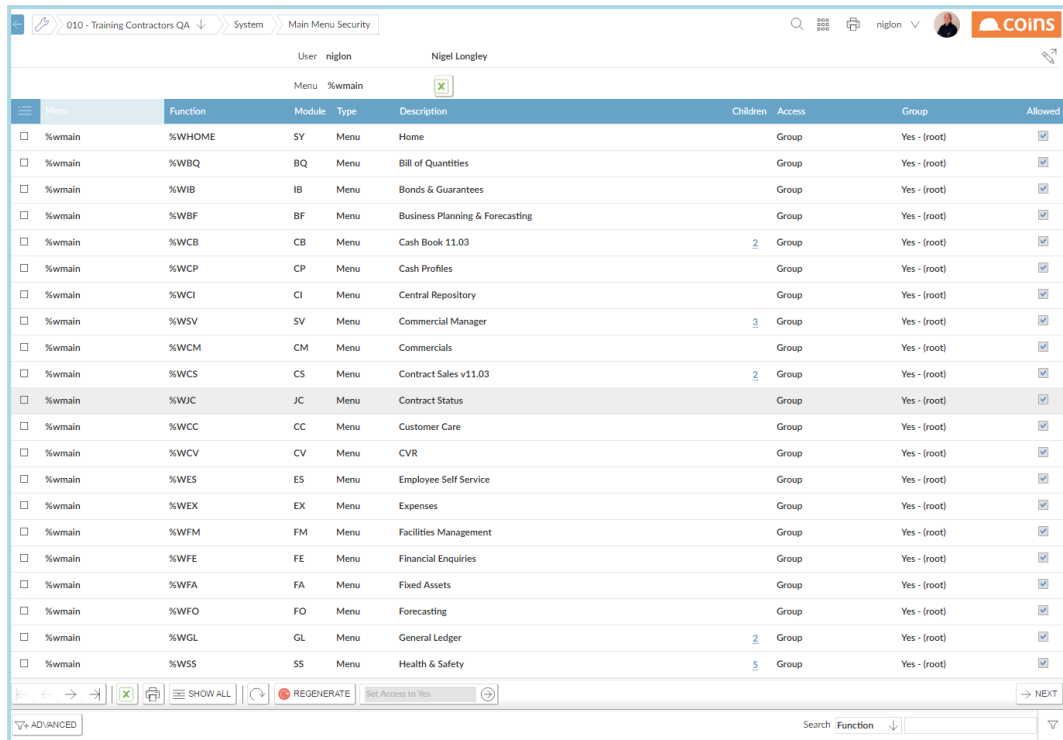
Navigate to System > User Maintenance > Function Security > Main Menu Security.



Select the group from the User/Group lookup and the top-most menu you want to assign to the group. Menu headings start with %W and are logical with the exception of house sales which is %WHS2. Some examples are shown below:

Cash Book	%WCB	Human Resources	%WHR
Company Information	%WCI	Plant	%WPC
Contract Sales	%WCS	Purchase Ledger	%WPL
Contract Status	%WJC	Procurement	%WPO
Expenses	%WEX	Subcontract	%WSC
Fixed Assets	%WFA	Sales Ledger	%WSL
Fleet Manager	%WFL	Site Manager	%WSM
General Ledger	%WGL		

Once you have made your selections, click Next.

Menu	Function	Module	Type	Description	Children	Access	Group	Allowed	
<input type="checkbox"/>	%wmain	%WHOME	SY	Menu	Home		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WBQ	BQ	Menu	Bill of Quantities		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WIB	IB	Menu	Bonds & Guarantees		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WBF	BF	Menu	Business Planning & Forecasting		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCB	CB	Menu	Cash Book 11.03	2	Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCP	CP	Menu	Cash Profiles		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCI	CI	Menu	Central Repository		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WSV	SV	Menu	Commercial Manager	3	Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCM	CM	Menu	Commercials		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCS	CS	Menu	Contract Sales v11.03	2	Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WJC	JC	Menu	Contract Status		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCC	CC	Menu	Customer Care		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WCV	CV	Menu	CVR		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WES	ES	Menu	Employee Self Service		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WEX	EX	Menu	Expenses		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WFM	FM	Menu	Facilities Management		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WFE	FE	Menu	Financial Enquiries		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WFA	FA	Menu	Fixed Assets		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WFO	FO	Menu	Forecasting		Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WGL	GL	Menu	General Ledger	2	Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/>	%wmain	%WSS	SS	Menu	Health & Safety	5	Group	Yes - (root)	<input checked="" type="checkbox"/>

Tick the required menus and select the required access value from the Choose Action drop-down box; press the Apply Action button:

The access options are as follows:

- No = the user does not have access to this function.
- Yes = If you are using Menu Item Security, the user has read-only access to this function. If you are not using Menu Item Security, the user has access to this function.
- Yes - Update = If you are using Menu Item Security, the user has update access to this function. If you are not using Menu Item Security, the Yes - Update option is not available.
- Group = The user's access depends on the permissions of the groups to which the user belongs.



Menu Item Security is a configurable option that allows you to control function access security at the level of items on COINS OA menus, and to specify update or read-only access.

If the parameter SY/MENUSEC = Y:

- If you grant access to a menu item, users have access to all its children, by default.
- You can specify read-only or update access to functions. The extra option (Yes-Update) is available in System > User Maintenance > Function Security > Main Menu Security and elsewhere.
- Users automatically have access to all functions with access type SYS, in all modules.
- Users automatically have access to menus if they have access to a function on the menu (this also applies to tabs and container functions).

To update access for several functions at the same time, select one or more records and either:



- Use the Choose Action menu or multiple update button to set the same access for all the selected menu items.
- Use the CONCURRENT Update button to set the access for each item separately.

To update access for a single function, use the OPEN button.

You can set the access for child functions by clicking the link in the Child column, and using the Choose Action to set the permissions for individual child functions. If you are using Menu Item Security, by default, the access to any child functions will be the same as the access to the parent function; setting them on this screen will override this default setting.

To check the access from a user perspective, assign the group to a user and log in as the user to view the assigned menus:



4.3.1.1 Main Menu Security Exclusions

When using main menu security (SY/MENUSEC=Y) then when access to a function is checked if the function is NOT a main menu function then it is checked using the Read Only and Update indicator.

Each function of this type has an attribute which specifies which main menu item it belongs to and whether it is a read only capability or an update capability. If the user has read only access to the main menu item then they also are granted access to the read only sub functions. If they have update access then they are granted both read only and update access to the sub functions.

This access can be modified by setting specific access for the desired functions. If specific access is defined then this is used in preference to the main menu security read only/update access described above.

This is now modified as follows. If the decision comes down to a read only/update access on a sub function to a main menu item then if the function is one of the six types specified in below and set in the parameter value then access will be denied.

From 11.04 the capability was added to change the default access for a main menu item from Y-YES to G-Group (so that further groups are then checked).

A new system parameter has been added

MENUEXC Main Menu Exclude Function Types

This will be a comma separated list of function types that should be excluded from the main menu security access model.

- A=Add
- B=Bulk
- C=Concurrent
- D=Delete
- X=Export
- U=Update

So setting SY/MENUEXC to B,D would mean that main menu security would not allow access to Bulk and Delete functions at all. If bulk and delete options are required then they would have to be specifically granted access in normal group security access (or user security access although this is not recommended).



4.3.1.2 Main Menu Security Exclusions Example

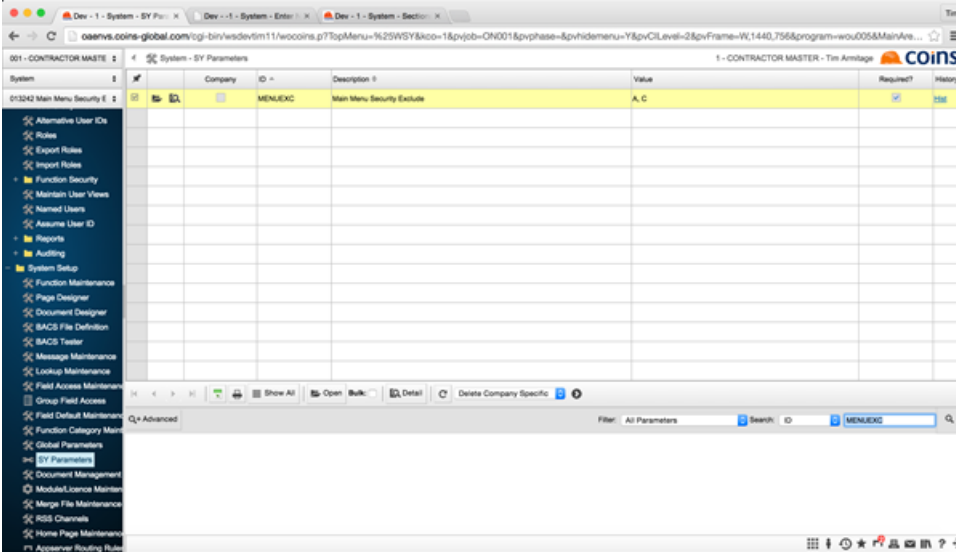
A user with access to the %WSYBMSF function in update mode

Function	Description	Module	Type	Category	Access
%WSYBMSF	Function Maintenance	SY	FUNCTION	MNT	Yes-Update
%WSYBMSFA	Add Function	SY	FUNCTION	MNT	Group
%WSYBMSFB	Bulk Maintenance	SY	FUNCTION	MNT	Group
%WSYBMSFC	Concurrent	SY	FUNCTION	MNT	Group
%WSYBMSFD	Delete	SY	FUNCTION	MNT	Group
%WSYBMSFU	Update Function	SY	FUNCTION	MNT	Group
%WSYBMSFX	Export	SY	FUNCTION	MNT	Group

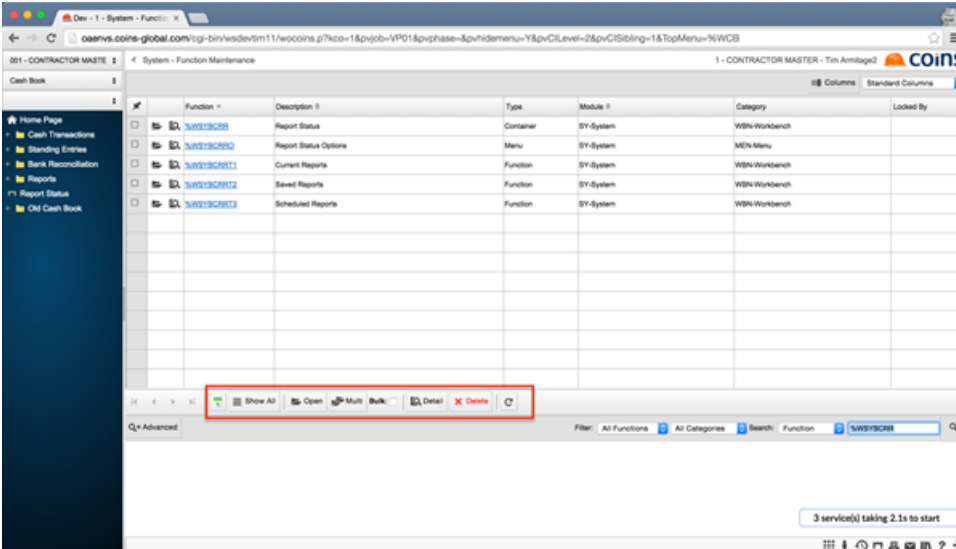
With SY/MAINEXC blank results in a normal updateable function

Function	Description	Type	Module	Category	Locked By
%WSYBMSF	Report Status	Container	SY-System	WBN Workbench	
%WSYBMSFA	Report Status Options	Menu	SY-System	WBN Menu	
%WSYBMSFB	Current Reports	Function	SY-System	WBN Workbench	
%WSYBMSFC	Saved Reports	Function	SY-System	WBN Workbench	
%WSYBMSFD	Scheduled Reports	Function	SY-System	WBN Workbench	

If MAINEXC is set to A,C then the Add and Concurrent buttons are suppressed.

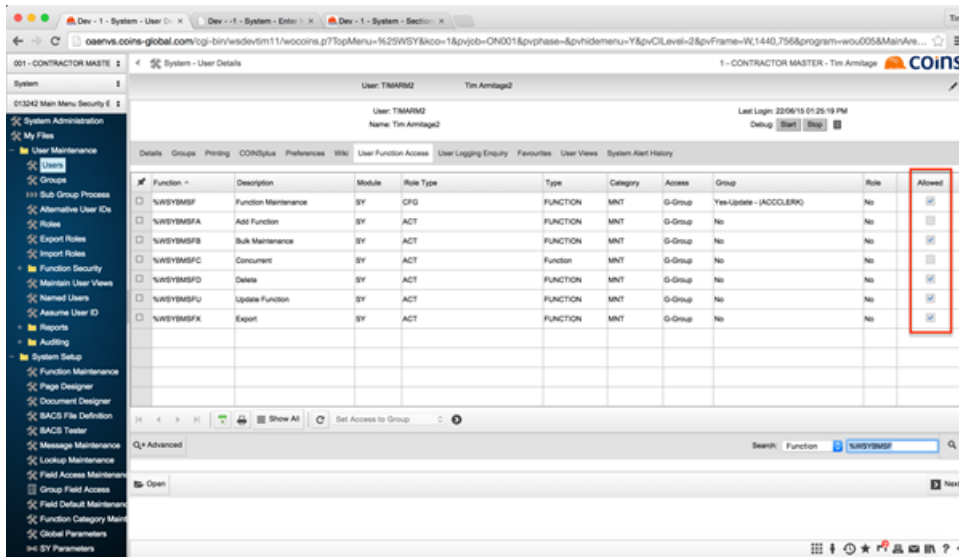



System	Company	ID	Description	Value	Required?	History
001 - CONTRACTOR MASTER	013042 Main Menu Security	MENUEXC	Main Menu Security Exclude	A.C	[checked]	



Function	Description	Type	Module	Category	Locked By
\WS\SC208	Report Status	Container	SY-system	WBN Workbench	
\WS\SC209	Report Status Options	Menu	SY-system	MEN Menu	
\WS\SC2091	Current Reports	Function	SY-system	WBN Workbench	
\WS\SC2092	Saved Reports	Function	SY-system	WBN Workbench	

The user access rights show the correct functions allowed

001 - CONTRACTOR MASTER

System - User Details

User: TINARIM2
Name: Tin Amilage2

Last Login: 23/06/15 01:25:19 PM
Debug [Start] [Stop]

Details Groups Printing CON2Plus Preferences Btl

User Function Access User Logging Enquiry Favoursites User Views System Alert History

Function	Description	Module	Role Type	Type	Category	Access	Group	Role	Allowed
✓ %WSYBMSF	Function Maintenance	SY	CFG	FUNCTION	MNT	G-Group	Yes Update - (ACCOLERK)	No	<input checked="" type="checkbox"/>
✓ %WSYBMSFA	Add Function	SY	ACT	FUNCTION	MNT	G-Group	No	No	<input checked="" type="checkbox"/>
✓ %WSYBMSFB	Bulk Maintenance	SY	ACT	FUNCTION	MNT	G-Group	No	No	<input checked="" type="checkbox"/>
✓ %WSYBMSFC	Consistent	SY	ACT	FUNCTION	MNT	G-Group	No	No	<input checked="" type="checkbox"/>
✓ %WSYBMSFD	Delete	SY	ACT	FUNCTION	MNT	G-Group	No	No	<input checked="" type="checkbox"/>
✓ %WSYBMSFU	Update Function	SY	ACT	FUNCTION	MNT	G-Group	No	No	<input checked="" type="checkbox"/>
✓ %WSYBMSFX	Export	SY	ACT	FUNCTION	MNT	G-Group	No	No	<input checked="" type="checkbox"/>

Search: Function %WSYBMSF

Open



4.3.2 Add Functions to Menu Headings using Interactive Security Update

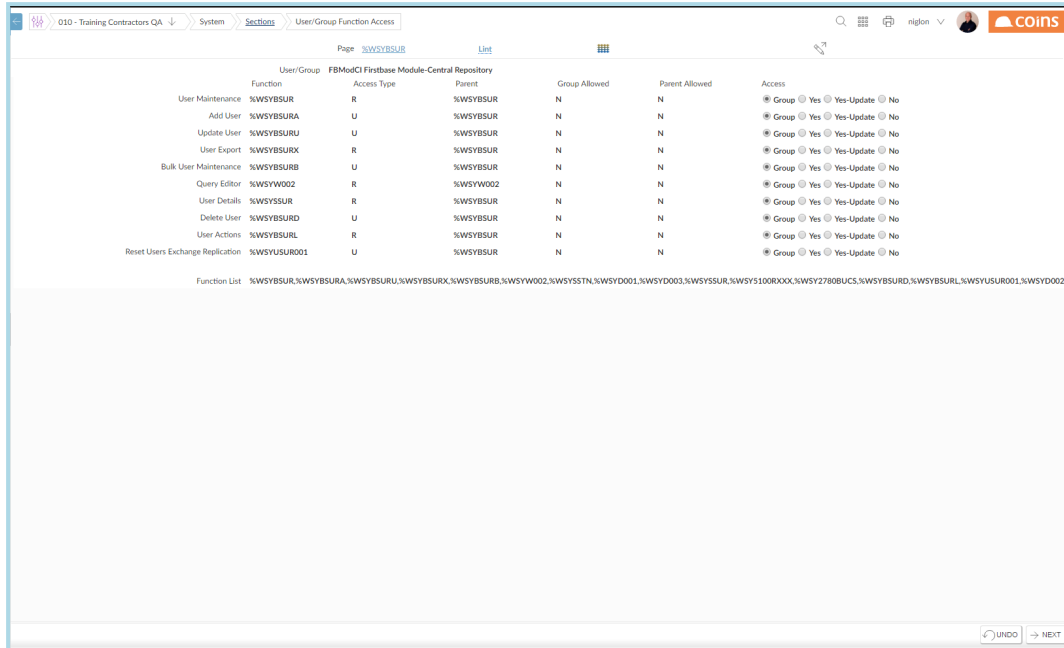
Interactive Security switches on interactive mode so that any screen you select will display an additional window containing associated functions for the active screen. This allows you to set the access for the group as you navigate around the system.

From the System menu select **User Maintenance > Function Security > Interactive Security Update**

User/Group	Name	Group?
FBAdmGL	Firstbase Administration-General Ledger	<input checked="" type="checkbox"/>
FBAdmPL	Firstbase Administration-Purchase Ledger	<input checked="" type="checkbox"/>
FBAdmSC	Firstbase Administration-Subcontract Ledger	<input checked="" type="checkbox"/>
FBAdmSL	Firstbase Administration-Sales Ledger	<input checked="" type="checkbox"/>
FBModBQ	Firstbase Module-Bill of Quantities	<input checked="" type="checkbox"/>
FBModCB	Firstbase Module-Cash Book	<input checked="" type="checkbox"/>
FBModCBV	Firstbase Module-VAT	<input checked="" type="checkbox"/>
FBModCC	Firstbase Module-Customer Care	<input checked="" type="checkbox"/>
FBModCI	Firstbase Module-Central Repository	<input checked="" type="checkbox"/>
FBModCM	Firstbase Module-Commercials	<input checked="" type="checkbox"/>
FBModCP	Firstbase Module-Cash Profiles	<input checked="" type="checkbox"/>
FBModCS	Firstbase Module-Contract Sales	<input checked="" type="checkbox"/>
FBModCV	Firstbase Module-CVR	<input checked="" type="checkbox"/>
FBModES	Firstbase Module-Employee Self Service	<input checked="" type="checkbox"/>
FBModFA	Firstbase Module-Fixed Assets	<input checked="" type="checkbox"/>
FBModFE	Firstbase Module-Financial Enquiries	<input checked="" type="checkbox"/>
FBModFM	Firstbase Module-Facilities Management	<input checked="" type="checkbox"/>
FBModFO	Firstbase Module-Forecasting	<input checked="" type="checkbox"/>
FBModGL	Firstbase Module-General Ledger	<input checked="" type="checkbox"/>
FBModHR	Firstbase Module-Human Resources	<input checked="" type="checkbox"/>
FBModHS	Firstbase Module-House Sales	<input checked="" type="checkbox"/>
FBModIB	Firstbase Module-Bonds & Guarantees	<input checked="" type="checkbox"/>
FBModIN	Firstbase Module-Inspections	<input checked="" type="checkbox"/>

Select the User/Group hyperlink of the group to which you want to add functions:

The following screen will be displayed.

User/Group	Function	Access Type	Parent	Group Allowed	Parent Allowed	Access
%WSYBSUR	User Maintenance	R	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	Add User	U	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	Update User	U	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	User Export	R	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	Bulk User Maintenance	U	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	Query Editor	R	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	User Details	R	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	Delete User	U	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	User Actions	R	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No
%WSYBSUR	Reset Users Exchange Replication	U	%WSYBSUR	N	N	<input checked="" type="radio"/> Group <input type="radio"/> Yes <input type="radio"/> Yes-Update <input type="radio"/> No

Function List %WSYBSUR,%WSYBSURA,%WSYBSURL,%WSYBSURX,%WSYBSURB,%WSYW002,%WSYSSTN,%WSYD001,%WSYD003,%WSYSSUR,%WSY100R00X,%WSY2780BUCS,%WSYBSURD,%WSYBSURL,%WSYUSUR001,%WSYD002

UNDO NEXT


Click Next, you will be returned to the previous screen

Navigate through the system as the user. Each area you select will display a screen similar to the screen above, enabling you to grant/deny function access to the group



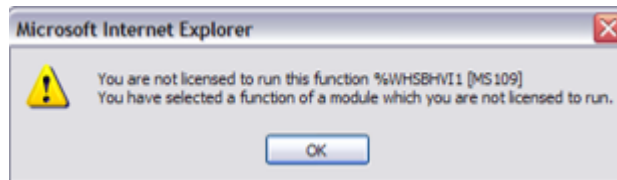
4.3.2.1 To Remove Interactive Mode

Delete &permuser=... from the url or log out and log back in to COINS

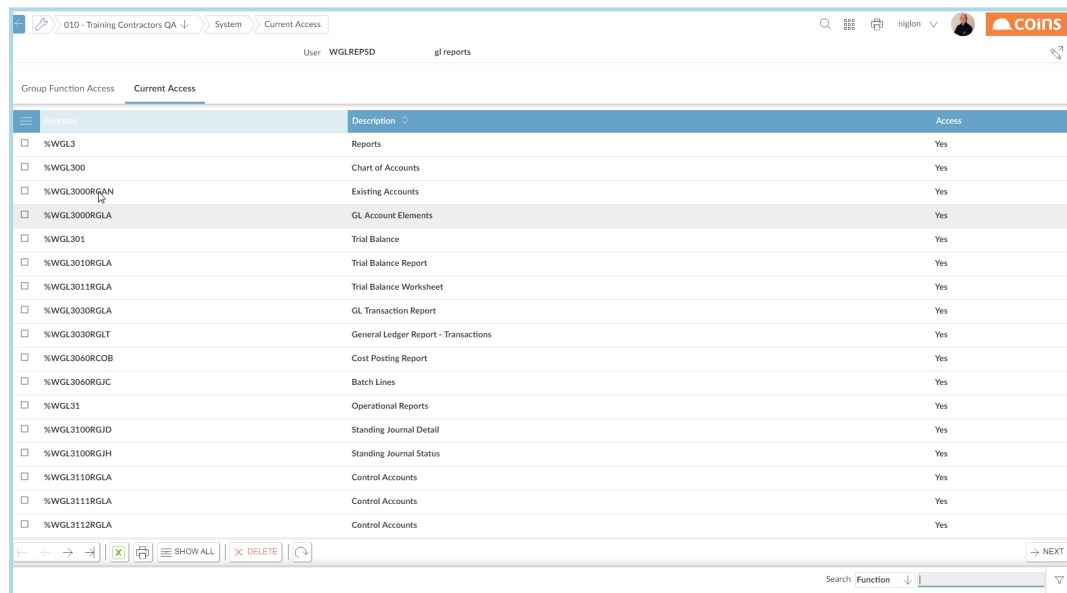
 pvCIlevel=2&program=wou005.p&sysuserRowid=0x000000000009d976&MainArea=%W5YBSUR&permUser=TDTEST

4.3.3 Find Functions

While setting up groups, you may find you have missed a function. A message similar to the one shown below will be displayed:



- Navigate to Groups and find the group that is granting access. The Current Access tab shows the functions you have given this group.



- From the Group Function Access tab search for the missing function. Tick the function you want to give access and from the Choose Action drop-down, select Yes and Apply Action.



010 - Training Contractors QA System Group Function Access

User: WGLREPSD gl reports

Group Function Access Current Access

Function	Description	Module	Type	Category	Access
<input type="checkbox"/> %WSYFSFF1	Move Document Field	SY	Function	MNT	Group
<input type="checkbox"/> %0	Financials	GL	Menu	MEN	Group
<input type="checkbox"/> %3580RPGLT1	Sort and Mode	PO	Function	REP	Group
<input type="checkbox"/> %APDEMO	Suppliers (ap_vendor)	SY	Return	WBN	Group
<input type="checkbox"/> %ATTAIL	SY Attribute Parameters	SY	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-A	C/B Audit Setup	CB	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-B	CO Audit Setup	CO	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-C	C/S Audit Setup	CS	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-D	EX Audit Setup	EX	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-E	GL Audit Setup	GL	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-F	JC Audit Setup	JC	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-G	PL Audit Setup	PL	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-GR	PL Audit Setup (Record Level)	PL	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-H	CIS Audit Setup	CI	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-I	PO Setup	PO	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-J	PR Audit Setup	PR	Function	CFG	Group
<input type="checkbox"/> %AUDTAIL-K	SC Audit Setup	SC	Function	CFG	Group

ADVANCED Search Function



4.3.4 Deny Access to Individuals

Where, for example, you have set up a group for your users but there may be a user or users that you want to deny some of the functions. Select the user from User Maintenance and find the function you want to deny them and set the access to N.

You can hide from groups or from individuals. The following example removes an export button from an individual's screen. First of all you need to find the function:

- Press Ctrl+Shift+Click the COINS logo on the top right of the screen and scroll down until you come to the list of functions Used. A screen is displayed showing functions for the screen you have displayed

COINSInfo Show All Hide All + Debug Messages + Web Variables + System Alert History + Functions/Sections + SectionFields + Parameters and Variables - Functions Used			
Function		Accessed Functions	
		Description	Context
%WPL1010BCOB	Invoice Batches		Enter Invoices
%WPL1010BCOBA	Add Invoice Batch		Add Batch
%WPL1010BCOBU	Update Invoice Batch		Update Batch
%WPL1010BCOBX	Export		Export
%WSYSSTN	Page Summary		Page Summary
%WPL1010SCOB	Invoice Batch		Batch
%WSY2000SSYN	(notesDesc) Notes Notes]		(notesDesc) Notes Notes]
%WSY5100RXXX	(title)		(title)
%WPL1010BCOBD	Delete Invoice Batches		Delete Batches
%WSY1010BCOBL	Batch Actions		Batch Actions
%WSY1013UCOB	Post Batches		Post
%WSY1014UCOB	Post Batches with Report		Post with Report
%WSY1015UCOB	Post GL Batches		Post
%WSY1016UCOB	Post GL Batches with Report		Post with Report
%WSY1017UCOB	Batch Posting/Listing Report		Posting/Listing Report
%WSY1018UCOB	GL Batch Posting/Listing Report		Posting/Listing Report
%WLM1981FCOB	Print Invoices		Print Invoices
%WPC1120FCOB	Charge Print		Charge Print
%WSC1160FCOB	Print RCTDCs		Print RCTDCs
%WSY1019UCOB	Cancel Batches		Cancel
Function List			
%WPL1010BCOB,%WPL1010BCOBA,%WPL1010BCOBU,%WPL1010BCOBX,%WSYSSTN,%WPL1010SCOB,%WSY2000SSYN,%WSY5100RXXX,%WPL1010BCOBD,%WSY1010BCOBL,%WSY1013UCOB,%WSY1014UCOB,%WSY1015UCOB,%WSY1016UCOB,%WSY1017UCOB,%WSY1018UCOB,%WLM1981FCOB,%WPC1120FCOB,%WSC1160FCOB,%WSY1019UCOB			

- Highlight and copy the function you want to hide.
- Navigate to Users from User Maintenance and select the User ID hyperlink for the user you wish to maintain.
- Select the User Function Access Tab



010 - Training Contractors QA System User Details

User: afsmir Afsaneh Mirazimi

User: afsmir Last Login: 19/10/15 14:58:53

Name: Afsaneh Mirazimi Debug: [START] [STOP]

Details Groups Printing COINsPlus Preferences Wiki **User Function Access** User Logging Enquiry Favourites User Views System Alert History

Function	Description	Module	Role Type	Type	Category	Access	Group	Allowed
<input type="checkbox"/> %WSYFSFF1	Move Document Field	SY		Function	MNT	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %0	Financials	GL		Menu	MEN	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %3580RPGLT1	Sort and Mode	PO		Function	REP	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %APDEMO	Suppliers (ap_vendor)	SY		Return	WBN	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %ATTAIL	SY Attribute Parameters	SY		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-A	C/B Audit Setup	CB		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-B	CO Audit Setup	CO		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-C	C/S Audit Setup	CS		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-D	EX Audit Setup	EX		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-E	GL Audit Setup	GL		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-F	JC Audit Setup	JC		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-G	PL Audit Setup	PL		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-GR	PL Audit Setup (Record Level)	PL		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-H	CIS Audit Setup	CI		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>
<input type="checkbox"/> %AUDTAIL-I	PO Setup	PO		Function	CFG	G-Group	Yes - (root)	<input checked="" type="checkbox"/>

ADVANCED Search: Function

OPEN NEXT

● Paste the function in the search field and set the access to No

010 - Training Contractors QA System User Details

User: afsmir Afsaneh Mirazimi

User: afsmir Last Login: 19/10/15 14:58:53

Name: Afsaneh Mirazimi Debug: [START] [STOP]

Details Groups Printing COINsPlus Preferences Wiki **User Function Access** User Logging Enquiry Favourites User Views System Alert History

Function	Description	Module	Role Type	Type	Category	Access	Group	Allowed
<input checked="" type="checkbox"/> %W2CB00	Cash Book Old	CB		Menu	MEN	G-Group	Yes - (root)	<input checked="" type="checkbox"/>

ADVANCED Search: Function %W2CB00

OPEN NEXT

● Click Apply Action.



4.3.5 Hide Tabs

The best way to find functions for tabs is to use &helpmode=prompt. Type this at the end of the URL.

Tab functions end with T and a number e.g. T6, T7 see screenshot below:

The screenshot shows the COINS Supplier Details page for Supplier ABB001. The main content area displays the supplier's information, including the name 'Abbey Glass', address '42 Bramall Lane, Sheffield, S25 4DL (SHEFFIELD)', and contact details. On the right side, there is a 'COINS Help' sidebar. In this sidebar, the 'Main (%WPL2000BAVMT1)' entry is highlighted with a red box. Below this entry, there is a table with two columns: 'Field' and 'Description'. The table lists various fields and their descriptions, such as 'Supplier Account (avm_num)', 'Payee Name (avm_payee)', 'Name (avm_name)', 'Address (avm_add)', 'Postcode (avm_pcode)', and 'Search Name'.

Once you have found the function for the tab, from the System menu select User Maintenance and Groups and select the Group hyperlink (Group Function Maintenance).

Find the function and set it to Group.



4.3.6 Access to Fields

If a user has access to a database table (see Table Access Security), by default they have access to all the fields in that table. You can control the access that users have to specific fields, using Field Access Maintenance.

You can prevent a user from being able to see or access the field at all, or you can allow them only to view the field but not update it, or only to add new data but not change existing data.

You can control the access for an individual user, or for all users.

For example, if you only want two users to be able to update the Account Closed field on Purchase Ledger > Suppliers > Suppliers, you could set one Read Only access record for all users, and two Update access records for the users you want to be able to update the field:

4.3.6.1 Hiding Fields Across All Screens

First you need to find the field name of the text you want to hide:

- Type `&helpmode=prompt` at the end of the URL:

`0/cgi-bin/train.cgi/wocoins.p7TopMenu=%WHS2&co=3&sidmainhelp=232%2C*%2C0&pvCIlevel=2&helpmode=prompt`

- Navigate to the screen you want to make changes to and select the Side-frame Help button in the global shortcuts bar. select the Toggle Help option from the User Menu

Field	Description
Supplier Account (avm_num)	The supplier number.
Payee Name (avm_payee)	The name to appear on cheques and Inland Revenue documentation.
Name (avm_name)	The name of the supplier.
Address (avm_add)	The supplier's address.
Postcode (avm_pcode)	The supplier's postcode.

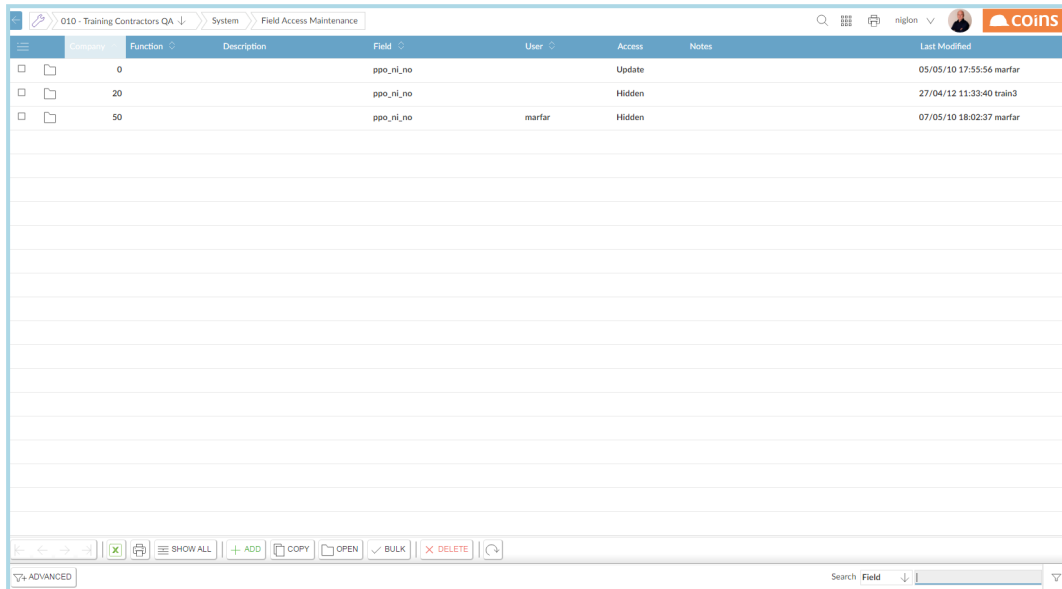
The field you require is now in the help screen. Highlight and copy the field name (the name shown within the brackets) you want to hide.

Navigate to **System, System Setup, Field Access Maintenance**.

Before you can hide a field you need to create a base record for Company 0.



- Select the Add button to add a new field and copy the field code and set the access to update.
- Now enter the company for which you want to change the access for the field. Select Hidden from the drop-down menu. Press Save.
- Add subsequent lines for the company(s) you want to hide.



Company	Function	Description	Field	User	Access	Notes	Last Modified
0			ppo_ni_no		Update		05/05/10 17:55:56 marfar
20			ppo_ni_no		Hidden		27/04/12 11:33:40 train3
50			ppo_ni_no	marfar	Hidden		07/05/10 18:02:37 marfar



If the function field is left blank, the field will be hidden in all occurrences

The example above shows all access to all companies except company 20 and 50

4.3.6.2 Group Field Access

You can also set up field access for groups:

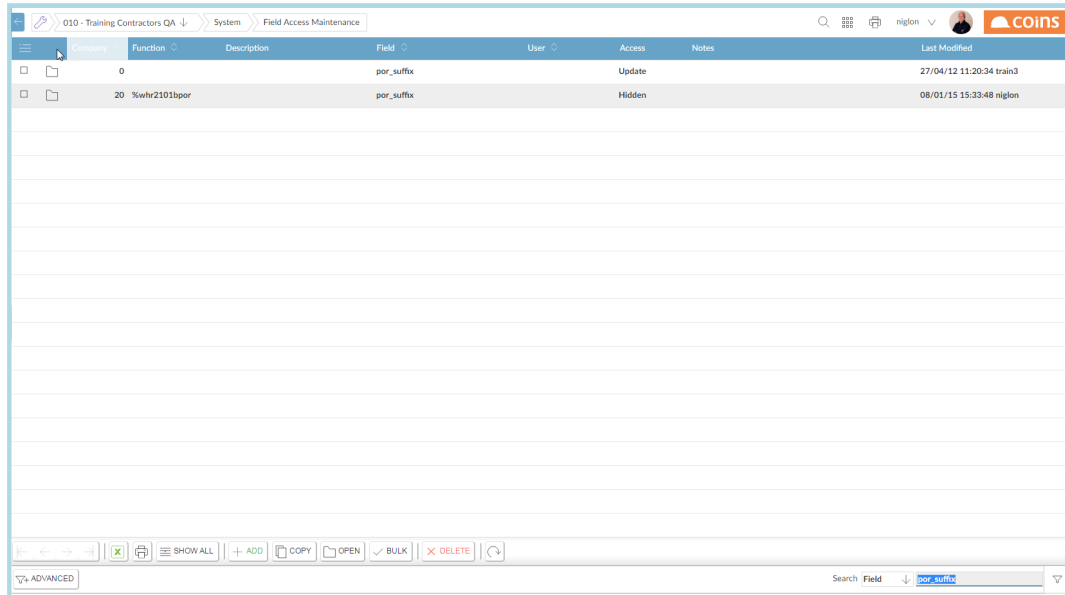
In **System > System Setup > Field Access Maintenance**, set up the access for the field, entering a group code in the User column.

Run **System > System Setup > Group Field Access** and select the group.

This creates a copy of the group's field access record for each user that belongs to the group.

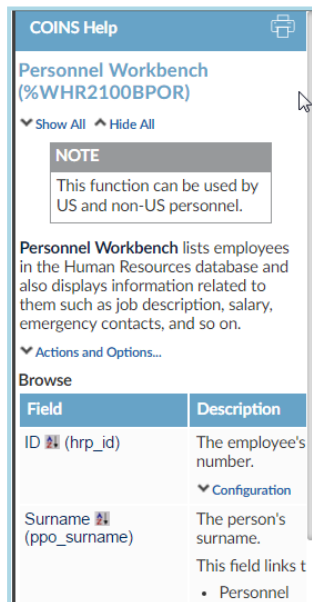
4.3.6.3 Hiding Fields in One Screen Only

If you only want to hide a field in this screen i.e. should this field be used anywhere else in Coins, it won't be hidden, only enter the function against the field - see example:



Function	Description	Field	User	Access	Notes	Last Modified
0		por_suffix		Update		27/04/12 11:20:34 train3
20 %wlr2101bpor		por_suffix		Hidden		08/01/15 15:33:48 niglon

You will find the function at the top of help screen &helpmode=prompt:



COINS Help

Personnel Workbench (%WHR2100BPOR)

▼ Show All ▲ Hide All

NOTE
This function can be used by US and non-US personnel.

Personnel Workbench lists employees in the Human Resources database and also displays information related to them such as job description, salary, emergency contacts, and so on.

▼ Actions and Options...

Browse

Field	Description
ID (hrp_id)	The employee's number.
Surname (ppo_surname)	The person's surname. This field links to • Personnel



4.4 Set Menu Security Utility - Overview

The Set Menu Security report provides a tool to report on, and if required update, all User Menu Access rights.

This functionality ONLY refers to Menu Function Security.

4.4.1 Business Reasons for Change

As part of COINS goal to improve overall user experience, one of the key activities from v11.04 has been to significantly redesign certain menu structures. The Set Menu Security report is intended to allow System Administrators to easily review and update the user menu access.

4.4.2 Initial Setup

No additional setup is required before using this function.



4.4.3 Set Menu Security - Screen and Processing Changes

Set Menu Security is available on the standard menus: **System > User Maintenance > Function Security**. The report only shows information on menu security NOT function security.

The report lists those menus on which a user or group has functions that they are allowed to run but which are on menus that are not currently available to them. It does not show any menus the user or group already has access to. The report is designed to show only the changes that will take place, not confirm what is already there.

The report operates in three modes: report, update and undo.

4.4.3.1 Report Mode

If you select Report mode, the following input fields are available:

User(s)/Group(s)

The Users and Groups you wish to check.

Root Menu

The root or top menu at which the report should start. Typically this would be the main module level such as %WGL or %WPO.

The report will return, for each user or group, the

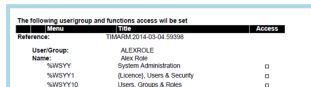
- The menu path checked.
- The menus that the user(s) or group(s) will be granted access to.
- Functions on these menus that the user(s) or group(s) currently have access to.



The following Usergroup and Functions access will be set			
Reference	UserGroup	Function	Access

4.4.3.2 Update Mode

If you select update mode, the same input fields are available. When run, the user(s) or group(s) are granted access to the menus as appropriate. The report provides a unique reference for the update as well as listing all menus to which the user(s) or group(s) have been assigned access.



The following Usergroup and Functions access will be set			
Reference	UserGroup	Function	Access
TIMARBL2014-03-04-55036	ALEXROLE	Admin Role	
	SWSYXX	System Administration	<input type="checkbox"/>
	SWSYXX	Business, Users & Security	<input type="checkbox"/>
	SWSYXX	Users, Groups & Roles	<input type="checkbox"/>

The unique reference, based on user, date and time, is used by the Undo Mode if necessary.



If the System Parameter UFACCESS is set, this must be reset following any changes made by this report

4.4.3.3 Undo Mode

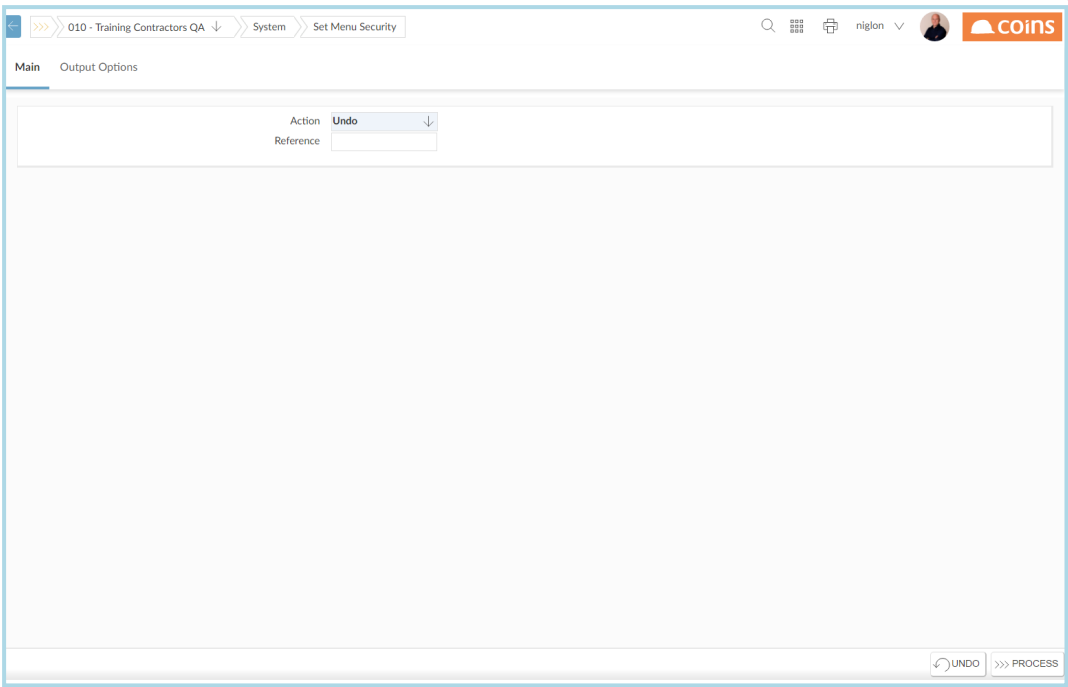
Undo Mode is ONLY designed to work before any other changes to any Function Access Security are made. The Undo Reference is only valid until the next reference is generated.

This functionality is purely designed to undo any errors rather than roll-back changes at a later date.

If you select Update mode, the following input field is available:

Reference

The reference number of the previous changes made.



The report returns a list, for each user/group, of the access changes which have been undone.

The following user/group and functions access will be set

Menu	Item	Access
Reference: TIMARM.2014-03-04.59398		
User/Group:	ALEXROLE	
Name:	Alex Role	
%WSYY	System Administration	<input type="checkbox"/>
%WSYY1	(Licence), Users & Security	<input type="checkbox"/>
%WSYY10	Users, Groups & Roles	<input type="checkbox"/>



5 Set Up a User

- From the System menu, select **User Maintenance > Users**

010 - Training Contractors QA > System > User Maintenance							
	User ID	Name	Prime Company	Companies	Security	Prime Group	Last Login
<input type="checkbox"/>	afamir	Afsaneh Mirazimi	10	*	9	Root	19/10/15
<input type="checkbox"/>	ALASPE	Alarm Specialist	0	*	0	Root	
<input type="checkbox"/>	andfar	Andy Farnfield	10	*	9	Root	20/05/11
<input type="checkbox"/>	andter	Andrey Terekhin	20	*	9	Root	18/10/11
<input type="checkbox"/>	ANDWAS	Andre Wasserman	10	*	9	Root	07/09/15
<input type="checkbox"/>	boball	bob allsorts	1	1	9	WMANDATORY	25/02/16
<input type="checkbox"/>	BrosnanP	Brosnan Pierce	10	10	9	Root	09/06/15
<input type="checkbox"/>	BTTrain	BTTrain	10	*	9	BTPROC	10/07/14
<input type="checkbox"/>	CARRIG	Carpet Rights Fitters	10	10	0	Root	
<input type="checkbox"/>	COINS	COINS User	0	*	9	root	
<input type="checkbox"/>	COINS3	COINS3	10	10	0		04/04/14
<input type="checkbox"/>	CollinsJB	Collins Jane Beverley	10	10	9	Root	04/10/11
<input type="checkbox"/>	ConneryS	Connery Sean	10	10	9	Root	04/10/11
<input type="checkbox"/>	CRYCLE	Crystal Cleaning	10	10	9	Root	01/08/11
<input type="checkbox"/>	danhar	Daniel Harrington	10	10	9	Daniel	10/07/14
<input type="checkbox"/>	davsch	David Schofield	10	*	9	Root	13/10/11
<input type="checkbox"/>	davyat	David Yates	20	*	9	Root	21/03/12
<input type="checkbox"/>	dhrbha	Dhruv Bhagat	10	*	9	ROOT	12/01/16
<input type="checkbox"/>	dhrbha1	dhruv	10	10	9	FBModPL	07/12/15
<input type="checkbox"/>	ECOELE	Eco Electricians	10	10	9	Root	01/08/11



You can copy an existing user's details. Tick the check box of the user to be copied and select the Copy button.

Maintain Users and Groups

5 Set Up a User



010 - Training Contractors QA

System

User Details

User

dhrrbha1

dhrruv

User

dhrrbha1

Last Login

07/12/15 11:00:59

Name

dhrruv

Debug

START

STOP

Details

Groups

Printing

COIN\$plus

Preferences

Wiki

User Function Access

User Logging Enquiry

Favourites

User Views

System Alert History

Setup

Password

Expires

Email

Domain\User

Extranet User

Restricted IP

Prime Group

Language

Prime Company

Companies

Security

Replication Mail Server

Replication Mailbox

Account Locked

☐

FBModPL-Firstbase Module-Purchase Ledger

None

10-Training Contractors QA

10

9

☐

Named User

Named User

Named Role

Designer

Compiler

Writer

Runner

ODBC Adapter

Webservices

Web Service

Companies

Workflow

Excel Server

☒

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

OPEN

NEXT



5.1 Details Tab

Enter the required information for the user in the Details tab:

Field	Description
User:	<p>Enter the user id. The user ID is the code which a person uses to identify themselves in the COINS system when logging in.</p> <p>Enter the Coins ID of the user. This is typically the first 3 digits of the first name and last name.</p>
Name:	The full name of the user with this ID.
Password	Enter the Coins password for the user. This can be changed by the user after login.
Expires:	<p>If used, enter the date this user's password will expire. After this date, the user will be forced to choose a new password before entering the system.</p> <p>If this is blank, the user's password will never expire.</p>
Email:	If this is entered it pulls through to the Activity WBN



Field	Description
Domain/User:	<p>The NT/Windows Domain name and user ID used for automatic login (for example, Coins/Sysadmin).</p> <p>The complete URL to the page which will perform the auto login request.</p> <p>Automatic login allows users to log in to COINS without entering a password, by using the Windows network login information. If WEBAUTO is blank then auto login will not be used and the users will need to login manually to COINS using the COINS user ID and password.</p> <p>The user's domain and user name must also be set correctly in the Domain\User field on the user record.</p> <p>A can-do list (a list in which wildcards are used to omit or include certain values. For example, !AB*, * means include all codes except those beginning "AB".) of IP addresses from which users can log in automatically (that is, without having to enter a password).</p> <p>If a user attempts to log in from an IP address that is not in this list, COINS will not attempt to log them in automatically. For example, you can use this to allow internal users to log in automatically but force someone logging in from an extranet to enter a password.</p> <p>The complete URL (Uniform Resource Locator - an Internet address that identifies a specific resource (such as a web site, file or directory). For example, http://www.coins-global.com/ is a URL) to the page which will perform the auto login request.</p> <p>Automatic login allows users to log in to COINS without entering a password, by using the Windows network login information. If WEBAUTO is blank then auto login will not be used and the users will need to login manually to COINS using the COINS user ID and password.</p> <p>The user's domain and user name must also be set correctly in the Domain\User field on the user record.</p>



Field	Description
Extranet User:	<p>Whether the user is an Extranet user.</p> <p>Extranet users are restricted to functions that are available to the user specified by the SY parameter EXTUSER user (if set) as well as their own security settings.</p> <p>If this field is not ticked, this user will not be able to log in from an IP address that is not specified by the SY parameter INTIPS.</p>
Restricted IP:	<p>The IP address(es) for this user.</p> <p>For example, this would be the address of the router from which the user accesses COINS. If specified, COINS only allows the user to log in if the IP address they are using is in this list. If blank then this user can use any IP address.</p> <p>Typically you would use this as an additional check on Extranet users, although you could also use it to restrict access by Intranet users (for example in different branches).</p>
Prime Group:	<p>The main group for this user. You are allowed to see another user's batches, reports etc if that users prime group is in your groups list and their security level is less than yours.</p>
Language:	<p>The language COINS uses for display when this user is logged in. 'None' means that COINS displays the default (UK English).</p>
Prime Company	<p>The company this user will connect to when first logging into COINS.</p>
Companies:	<p>A list of companies this user is allowed to access.</p> <p>For example:</p> <p>!4,* The user has access to all companies except company 004.</p>
Security:	<p>Only relevant to posting batches e.g. if you are set to level 8 you can post anyone's batches for those set at 7 and below</p>



Field	Description
Account Locked	<p>If this is ticked, it will be impossible for this user to log in using any interface.</p> <p>This field will be automatically ticked if:</p> <p>The user exceeds the number of login attempts as set by the LOGATTEM parameter.</p> <p>The user does not log in within the number of days set in the LKUNUSED parameter.</p>
Replication Mail Server	<p>Name of the mail server for which this user's appointments, tasks and email data are replicated</p> <p>For Exchange server replication (i.e. when IF/MAILREPL is set to E-Exchange) this field should contain name of the mail server and it needs to match environment name in the Exchange replication software configuration file.</p> <p>For Lotus Notes server replication (i.e. IF/MAILREPL is set to L-Lotus) set hard-coded value of "Lotus". If this field is left blank then replication is not enabled for this user..</p>
Replication Mailbox	<p>The name of the mailbox on the exchange server.</p> <p>If this is blank, the user ID will be used instead.</p>
Named User:	<p>Tick this field to give the user access to COINS. The number of current users you can have is limited by your licence.</p>
Designer:	<p>Tick this field if the user is licensed to run designer functions</p>
Writer:	<p>Tick this field if the user is licensed to run report writer functions</p>
ODBC Adaptor:	<p>Whether the user is licensed to access Webservices. These allow XML program requests from other systems. They are used for integration of 3rd party applications with COINS.</p>
Web Services:	<p>The number of users allowed to access Webservices is limited by your licence.</p>
Workflow	<p>Whether the user is licensed to run workflows.</p>
Excel Server	<p>Whether the user is licensed to run a report which is processed on an Excel server.</p>

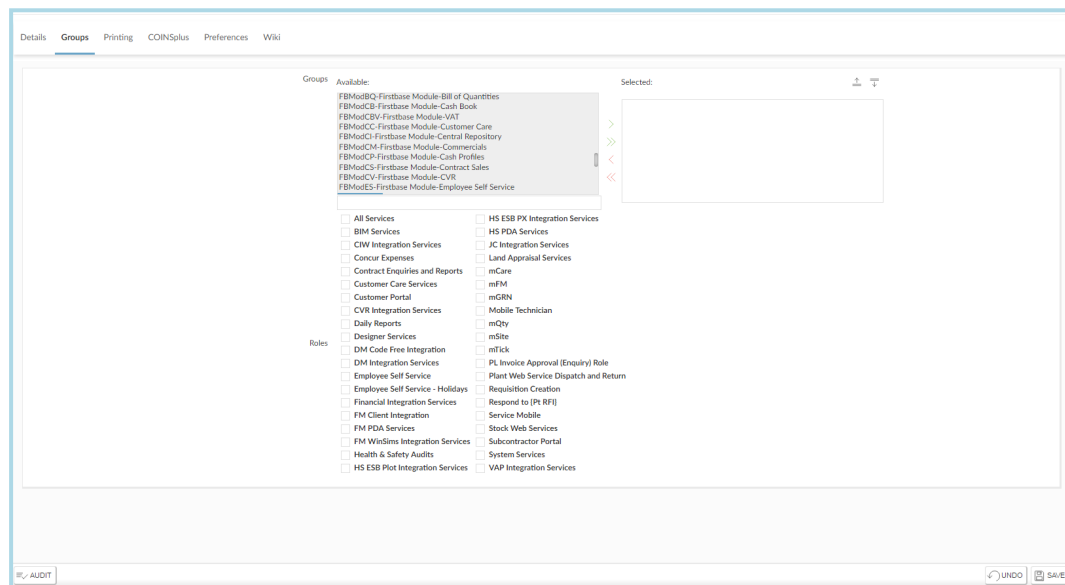


5.2 Groups Tab

5.2.1 Groups

Each user belongs to one or more groups. By default, users in the same group have access to the same subset of COINS menus and procedures. However, you can grant or deny individuals within a group access to different menus and procedures; they do not need to be restricted to the access permissions for the group.

Select the group you want to assign to the user from the Available field and use the green arrows to move the group(s) to the Selected Field. Red Arrows allow you to deselect groups from the selected field:



5.2.2 Roles

Many users will use only a few COINS functions and, maybe, only occasionally. Role-based licensing provides a cost-effective way of giving access for large numbers of users to small but important parts of COINS. Role-based licensing uses the concept of "named role" users; these do not count as regular concurrent licensed users. Your COINS licence determines the number of "named role" users you can have.

Roles are pre-defined by Construction Industry Solutions, and issued as part of standard data. Each role has a limited number of functions that it provides access to. Each "named role" user can be assigned to one or more roles (thus giving them access to one or more groups of functions); they will only be allowed to run the functions associated with those roles. You must give them access (using standard function access) to the top-level module menu for any functions they will need to run (for example, %WPL for any Purchase Ledger functions), but COINS automatically gives access to any submenus needed. You can use standard function access to prevent "named role" users from accessing specific functions within the role; however, you cannot grant them access to additional functions outside their role.



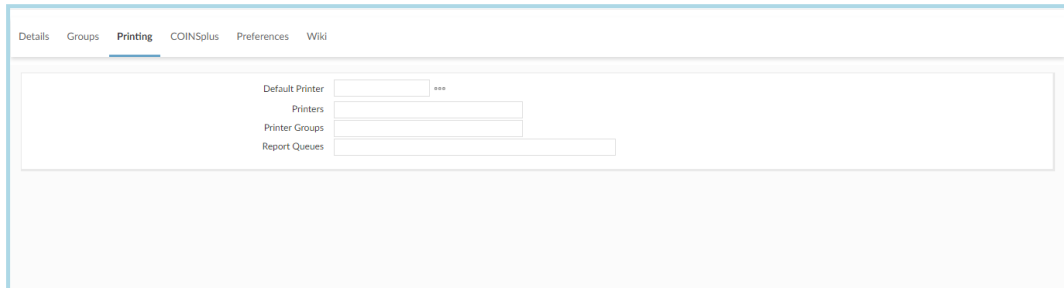
Named role users always have access to basic lookups, some system functions such as Home > Report Status and Home > Activity Workbench, and the documentation. See Access to Mandatory Functions.

You cannot change which standard (%) functions belong to a role, but you can add non-standard (that is, user-defined) functions to existing roles, up to the number allowed by your COINS licence.

Your COINS licence determines the maximum number of users you can assign a role to; you will not be able to assign a role to a user if that number of other users already have the role assigned to them.

5.3 Printing Tab

This tab allows you to specify which printers the user has access to.



Field	Description
Default Printer:	The default printer for this user.
Printer:	A list of printers the user is allowed to use.
Printer Groups:	A list of printer groups which the user is allowed to use. The group to which a printer belongs is set up in the Group field in Printer Maintenance. If the printer and group list are blank, the user can use all printers.
Default Queue:	Default report queue for the user.
Report Queues:	List of queues the user has permission to use. May contain wildcards.



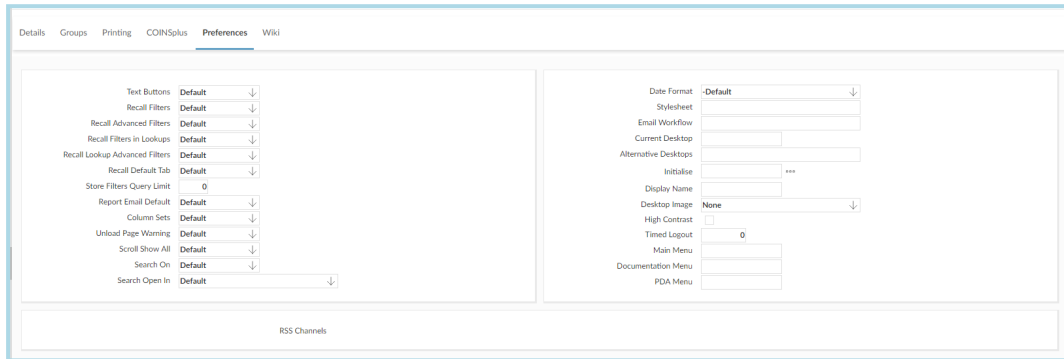
5.4 Coinsplus Tab

This tab allows you to set up features that control how this user uses the COINSplus interface. For OA only users, this tab is not required to be completed.

Field	Description
Root Menu	The code of this user's home menu. The home menu is the menu which this user will go to when they log in, or if they press Home.
Hot Menu	The code of the menu that is run if the user selects their hot menu option.
Hot Procedure	The code for a procedure which is run every time this user logs in.
Parameter	Any parameters that are required for the user's hot function.
Hot Print Menu	Whether this user is allowed to go directly to the printer menu by pressing P. If this is not ticked, when the user presses P they go directly to Maintain Queued Print Requests
Mail On	Whether COINS informs this user of incoming mail messages from other users. Users can change this setting using User Preferences.
Editor/Breakout	Whether this user is allowed access to the PROGRESS® editor. This also controls whether the user is allowed to run procedures (using " . "). Only give a user permission to use the editor if they are familiar with PROGRESS®; even so, they should only use the editor if instructed to by COINS.
Timed Logout	The number of minutes a user's process can remain idle at a menu before they are logged out automatically. If this value is 0, the process can remain idle indefinitely. This is subject to the maximum value set in Menu System Configuration.

5.5 Preferences Tab

This tab allows you to set preferences for this user.



Field	Description
Text Buttons	<p>Whether to show text, icons or both on buttons. This only affects selected buttons.</p> <p>Default take the value of the SY/PREFTEXT parameter</p>



Field	Description
Recall Filters	<p>How the filter preferences for this user should be recalled from previous sessions.</p> <p>Full = all filters are recalled</p> <p>Day = recall the filters from today only</p> <p>Session = only recalls from the current session</p> <p>None = does not recall filters</p> <p>Default takes the value of the SY/PREFFILT parameter.</p>



Field	Description
Recall Advanced Filters	<p>How the advanced filter preferences for this user should be recalled from previous sessions.</p> <p>This allows you to prevent advanced filter selections, which may result in a slow performing screen, from being retained.</p> <p>The options are:</p> <p>Full - Recalls all filters.</p> <p>Day - Recalls the filters from earlier today only.</p> <p>Session - Only recalls from the current session.</p> <p>None - Does not recall filters.</p> <p>Default - Uses the system default setting.</p> <p>The SY/PREFADV parameter determines the system default.</p>



Field	Description
Recall Filters in Lookups	<p>How the filter preferences for this user should be recalled from previous lookups.</p> <p>The options are:</p> <p>Full - Recalls all filters.</p> <p>Day - Recalls the filters from earlier today only.</p> <p>Session - Only recalls from the current session.</p> <p>None - Does not recall filters.</p> <p>Default - Uses the system default setting.</p> <p>Default takes the value of the SY/PREFFILT parameter.</p>




Field	Description
Recall Lookup Advanced Filters	<p>How the advanced filter preferences for this user should be recalled for lookups from previous sessions.</p> <p>This allows you to prevent advanced filter selections, which may result in a slow performing screen, from being retained.</p> <p>The options are:</p> <p>Full - Recalls all filters.</p> <p>Day - Recalls the filters from earlier today only.</p> <p>Session - Only recalls from the current session.</p> <p>None - Does not recall filters.</p> <p>Default - Uses the setting from the SY/PREFLADV parameter</p>



Field	Description
Recall Default Tab	<p>How the default tab to show should be set for this user.</p> <p>The options are:</p> <p>Full - Always shows the most recent tab that this user visited.</p> <p>Day - Shows the most recent tab that this user visited today.</p> <p>Session - Shows the most recent tab that this user visited during the current session.</p> <p>None - Always shows the first tab on the screen.</p> <p>Default - Uses the system default setting as set by the SY/PREFTAB parameter</p>
Store Filters Query Limit	<p>The time limit in milliseconds above which filter settings for browses will not be stored.</p> <p>This is used to prevent a combination of advanced filters and sort orders, which have taken too long to return a set of records, from being stored and used by default the next time the user visits the page. Instead, the default filter will be used.</p> <p>If left as zero, the system default value as determined by SY/PREFQLIM parameter is used.</p>



Field	Description
Report Email Default	<p>The default setting for the Email tick box on report selection.</p> <p>Set this to Yes if you want reports this user generates to be emailed to their email address by default.</p> <p>Default - Uses the system default setting as set by the SY/REMAIL parameter</p>
Column Sets	<p>Whether this user should be allowed to set up and use different columns on browse screens, where available.</p> <p>Column sets are alternative groups of columns to display on browse screens. They are not available on all screens, but if they are available and the user is allowed to use column sets,</p> <p>a  Columns button gives access to the column sets configuration function, and a drop-down selector at the top right of the screen allows the user to choose which column set to display.</p> <p>Default means use the value of the System parameter SY/COLSETS.</p>
Unload Page Warning	<p>Whether to show a warning if the user tries to move off a page where unsaved data might still be present.</p>



Field	Description
Scroll Show All	Whether to scroll "show all" pages.
Search On	Whether the global search feature is available for this user.
Search Open In	How links from the global search function should open (in what type of window/frame).
Date Format:	Select the preferred date format from the dropdown.
Stylesheet:	<p>User-specific stylesheet if required.</p> <p>This can be used override styles in the standard stylesheet and company-specific stylesheet; for example, to provide a contract/site style where the user s on a specific site.</p>
Email Workflow	<p>The workflow templates that should send actions to this user as an email (if configured).</p> <p>Enter a comma separated list of the workflow templates or Enter * for all workflow actions to be sent as emails.</p>

Field	Description
Current Desktop	<p>The desktop menu to be shown. If blank then the desktop is suppressed.</p> <p>Each user can have a different desktop, or several users can use the same desktop. Note that if the user has access to the Desktop tab in User Preferences, they will be able to modify the desktop, and any changes they make will apply to any other users who share that desktop.</p>
Alternative Desktop	<p>A comma-separated list of desktops to which this user has access (including the user's current desktop).</p> <p>If this field is populated, a selector at the top of the user's desktop will allow them to switch between the alternative desktops.</p>
Initialise	<p>The COINS calculation program that should be run for this user on initialisation of the desktop.</p>




Field	Description
Desktop Image	<p>The background image for the desktop.</p> <p>This background only applies to this user's view of the desktop; if users share the same desktop, they can have different background images.</p> <p>The images that are available as desktop backgrounds are in</p> <p>\$BASE/custimg/bg/.</p> <p>You can load images using System > System Setup > Background Images</p>
Timed Logout	<p>The number of minutes of inactivity before the user is logged out of the system.</p>
Main Menu	<p>The main menu that this user should be presented with on login. If left blank, then the standard main menu will be shown.</p> <p>The main menu is the list of modules that appears in the module selector in the menu frame. The user will be taken to the first module in this list.</p>



Field	Description
Documentation Menu:	The main menu that this user should be presented with by default, when they select the documentation module. If this is left blank then the standard documentation menu will be shown.
PDA Menu	<p>The main menu that this user should be presented with, by default, on login on a mobile device. If this is left blank then the standard main menu will be displayed.</p> <p>The main menu is the list of modules that the user can select from. The user will be taken to the first module in this list.</p>



Field	Description
RSS Channels	<p>The RSS channels that this user subscribes to.</p> <p>RSS allows you to view news headlines and other information from different websites in one place. In COINS, these can be displayed on the module home pages, or viewed using RSS Reader.</p> <p>If all tick boxes are blank, the user can view all channels in RSS Reader, but no channels will be included on the home pages.</p> <div>  <p>The channels must first be set up using RSS Channels in System Setup.</p> </div>



5.6 Wiki Tab

Wiki allows you to specify which Wiki webs the user is allowed to contribute to, and to read only.



The webs are defined using Wiki Webs and the Wiki tab only displays if a least one web has been defined.

Wiki Read:	Which Wiki webs the user is allowed to view.
Wiki Writer:	Which Wiki webs the user is allowed to update.



6 Removing a User

When you no longer want a user to have access to COINS (for example, when they leave the company), you should disable their User ID. However, you should not delete their user record; COINS has the policy of retaining details of all historical users in the database for the following reasons:

- Ensuring that the transactional audit trail retains details of who input and/or authorised transactions, orders, payment runs, etc;
- Ensuring that reprinted documents, including purchase orders, etc. will correctly print without missing information;
- Ensuring that there is referential integrity within the database where database records refer to user IDs;
- Preventing problems when users need to edit records which include reference to a user who has left (in some circumstances, if the details of the original user have been deleted then an error message will be displayed and the user will need to overwrite the original details with a current user): this can be both frustrating at the time and misleading for the future;
- Allowing access to the User Logging Enquiry to review functions used on COINS by the historical user (subject to the time limit set in SY parameter LOGHIST).



6.1 To disable a user in a secure manner:

Untick the Named User box in the Named User group of fields on the User Details screen. This will remove the user from the user count for licensing purposes and will disable their user ID so that they cannot log in.

As added security, various other settings on the user record could be changed as follows to further deny the possibility of them gaining any access (although none of these should be necessary if they are no longer recorded as a named user):

- All the groups could be removed from the user -- thus removing their function access and a Group called "LEAVER" could then be added to their user record as their prime group -- this group would be configured to have no function access;
- The user's password could be changed;
- The Domain\User field could be blanked (if this is used);
- The Restricted IP field could be set (preventing login from any other IP address);
- Delete the User Views for this user (see User View Set Up).

You may want to consider other places in COINS where the user is referred to. For example:

- If the user is set up in the House Sales > Plot Sales > Setup > Sales Staff list in House Sales then this record should be marked as dormant.
- If the user is set up in the Procurement > Setup > People Information System > Buyers list in Procurement, this record should be marked as retired.



7 Run a User Report

The User Report allows you to produce a report that shows COINS users, the companies they have access to, and the user groups they belong to.

From the Systems menu, select **User Maintenance, Reports and User Report**.

- Select the User(s) to be reported on and click Next.
- The report will be generated and placed on the Report Status Workbench.

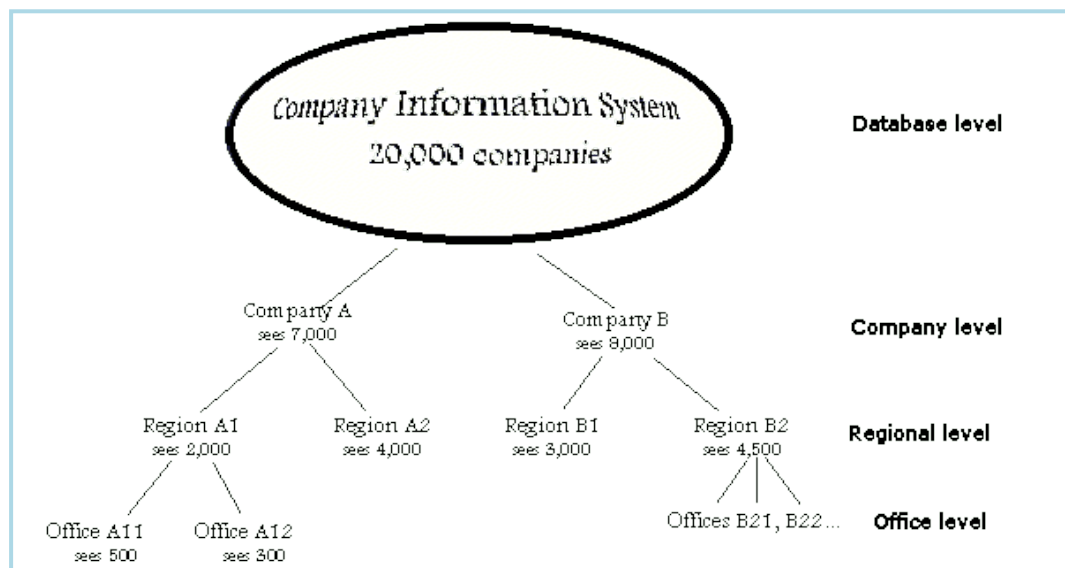
System - User Report
Training Contractors QA

User	Name	Primary Company	Other Companies	Primary Group	Other Groups	Security
sujeon	Sue Jones	10	*	Root	Root	9
sunava	Sunita Avadhani	40	*	Root	root	9
suzcha	Suz Chapman	20	*	Root	root	9
SYSAdmin	System Administrator	1	*	Root	root	9
TBA	TBA User for CC Scheduling	0	*	Root		0
test1	test1	20	20	wfminput	wfminput, wman	9
Test2	Test 2	10	20	FMINPUT	FMINPUT, man	0
test4	test four	20	20	FMINPOA	FMINPOA, GLINPOA, wman, #SYSADM	1
tester1	test change	10	*			0
tester2	test change3	10	*			0
testFM4	test four	20	20	OAFMGroup	GLINPOA, wman, #SYSADM, OAFMGroup	1
testuser	Test user	10	*	Root		9
TESTz	Afsaneh Mirazimi	10	*	Root	root	9
thaman	Thanya Mansfield	20	*	Root	root	0
timdaltid	Tim Drake Alternative Id	111	111	wplinp	wmandatory, wplinp, wplrep	0
timddm1	Tim Drake DM 1	101	101,111	Root	root	0
timddm2	Tim Drake DM 2	401	401,101	Root	root	0
timdplant	Tim Drake Plant Id	105	105	wplant	wmandatory, wplant	0
timdra	Tim Drake	101	101	Root	root	0
tonsta	Tony Starr	10	*	Root	Root	9
Train09	Train User 09	10	10	Root	Root	9
train1	Train 1	10	*	root	root	9
train10	ravi	10	*	Root	Root	9
Train11	Train User 11	10	10	Root	Root	9
Train12	Train User 12	10	10	Root	Root	9
Train14	Train User 14	10	10	Root	Root	9
Train15	Train User 15	10	10	Root	Root	9
Train16	Train User 16	10	10	Root	Root	9
Train17	Train User 17	10	10	Root	Root	9
Train19	Train User 19	10	10	HSSCADMIN	HFSCADMIN	9
train2	test change	10	*	Root	root	9
train3	Train 3	10	*	Root	root	9

8 User Views

User views allow different users to see different lists of companies and projects. For example, COINS may hold information about thousands of companies, but staff at a local office may only need to see companies that they deal with. Staff at a different local office may need to see a different list of companies, and staff at a regional office may need to see a larger list that includes all the companies visible to the local offices.

Views relate to an organisational hierarchy. For example:

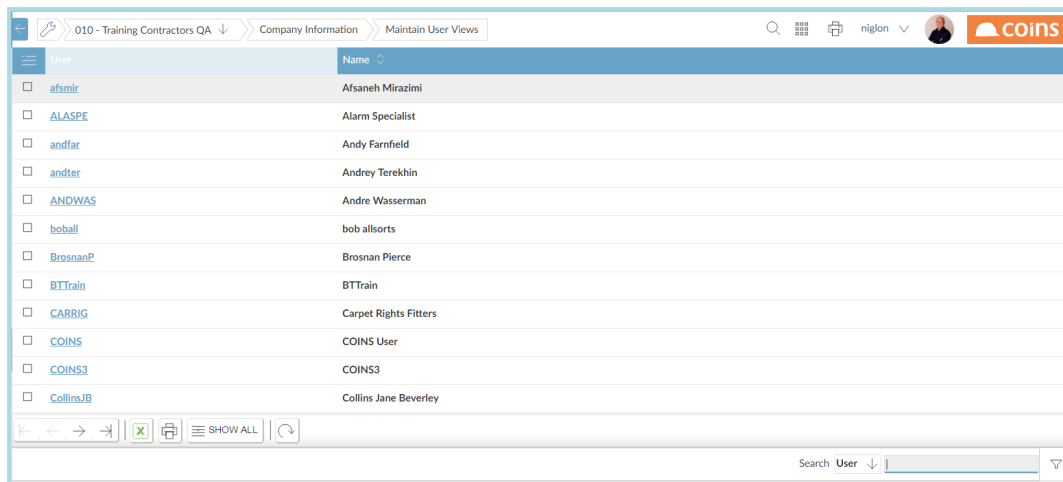


The names for the different levels (operating company, region, office in the example above) will depend on the way your system has been set up. You can have up to five levels. The top level view shows the entire database; the lowest view might be the site level. A view is based on a combination of the level and the entity at that level. For example, one view might be "Level 3 - Southern Region" and another view might be "Level 4 - Slough Office".

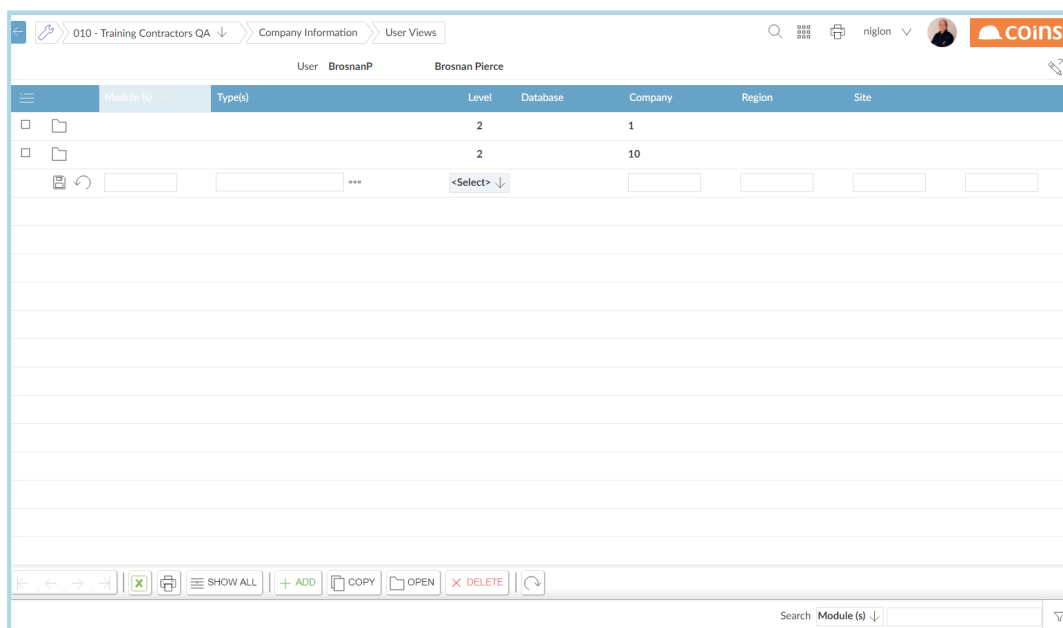
A user's view is the lowest level at which they are able to view the database. The user can always change their view to see the views at higher levels (for example a user whose view is "Level 4 - Slough Office" will be able to change their view to see the companies and projects that are visible in "Level 3 - Southern Region". They can add companies and projects from higher levels to their view.

In general, all users with the same view will see the same data. So if users Smith and Jones both have the Slough office view, and Smith adds a company to the view, Jones will also see that company. However, an individual user's view can be restricted to only see companies of certain types; for example, user Thomas may only need to see the suppliers that the Slough office deals with, and not subcontractors.

From the System module select **User Maintenance > Maintain User Views**


Select the hyperlink for the User and then click  button. Enter the details in the relevant fields.



Field	Description
Module(s):	The module for which you want to define the view for example PO or MK. Leave blank to define the same view for all modules.
Type(s):	Which type of company (for example, supplier, subcontractor) the user will see. Leave blank to see all types.



Field	Description
Level:	The number of the user's base level - their lowest (most restricted) view of the database.
Company:	A way of defining further the view that the User will see.
Region:	A way of defining further the view that the User will see.
Office:	A way of defining further the view that the User will see.
Contract;	A way of defining further the view that the User will see.

 Click 



9 Creating Buyers

The Buyers menu option allows you to create and maintain a list of people who are authorised to raise and/or commit purchase orders.

From the Procurement module select **Setup > People Information System > Buyers**.

A list of current buyers will be displayed.

Buyer's Code	Name	Department	Max. Order Value (Materials)	Max. Order Value (Plant)	Max. Order Value (Subcontract)	Retired
000500	FM Operative Fred		0	0	0	
alebak	Alex Balkushin		0	0	0	
alehul	Alexei Hukidov		0	0	0	
DAVSCH	David Schofield		0	0	0	
daavat	David Yates		50,000	50,000	50,000	
dhubha	Dhruv Bhagat		0	0	0	
ewahug	Ewan		500,000	500,000	500,000	
gabgon	Gabriel Gonzalez		0	0	0	
johcur	John Curtis		0	0	0	
jossrev	Joss Reveley		0	0	0	
karmas	Karen Mason		500,000	500,000	500,000	
kerbro	Kerry Brown		10,000	0	0	
leeebb	Lee Ebbrell		0	0	0	
nadgan	Nadya Garicheva		0	0	0	
NATANT	Natalia Antonova		0	0	0	
niglon	Nigel Longley		0	0	0	
niksil	Nikolai Silkin		0	0	0	
petfor	Peter Forrest		0	0	0	
ricare	Richard Preston		0	0	0	
sanhou	Sandra Hougham		0	0	0	

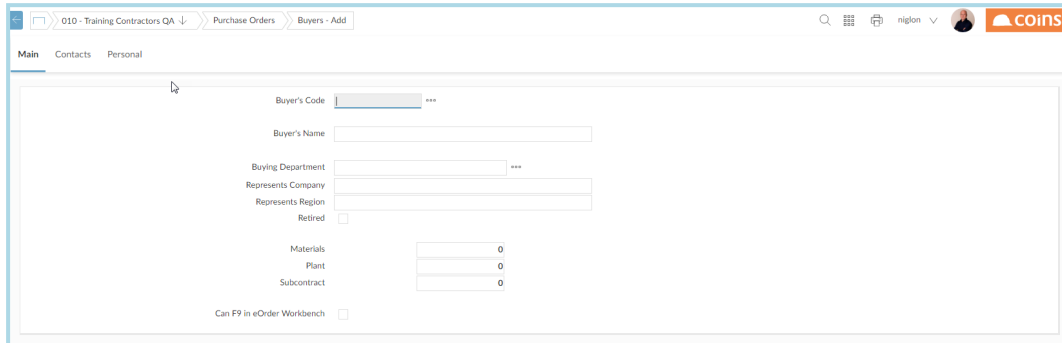


Click **ADD** and enter the details in the relevant fields.



Click **SAVE** when entry is complete

9.1 Main Tab



Field	Description
Buyers Code:	The User ID of the buyer.
Buyers Name:	The name of the buyer.
Buying Department:	The buying department.
Represents Company:	The company that the buyer represents. This is memorandum text only and can be printed on the purchase order
Represents Region:	The region that the buyer represents. . This is memorandum text only and can be printed on the purchase order
Retired:	<p>Whether this buyer is retired.</p> <p>You can prevent retired buyers from raising or committing orders.</p> <p>Associated Parameters</p> <p>PO/BUYERVAL</p>
Materials:	The maximum value that the buyer is allowed to order on material orders.
Plant:	The maximum value that the buyer is allowed to order on plant orders.
Subcontract:	The maximum value that the buyer is allowed to order on subcontract orders.
Can F9 in the eOrder Workbench:	Select this if the buyer is allowed use the F9 option in coinsplus in the eOrder Workbench.



9.2 Contacts Tab

Field	Description
Email:	The email address of the buyer.
Telephone:	Telephone numbers for this buyer.
Fax:	The fax numbers for the buyer.
Pager:	Pager numbers for this buyer.



9.3 Personal Tab

Field	Description
Personal Reference Number:	Memorandum text only. Maximum Length: 20 characters
Position in Company:	Memorandum text only. Can be printed on the Purchase Order. Maximum Length: 50 characters
Specialist Areas of Knowledge:	Text to identify particular areas of knowledge this buyer has. Memorandum text only. Maximum Length: 100 characters



10 Contract Security

Using contract security, you can control which users are allowed access to which contracts.

If a user is denied access to a contract, they will be unable to enter transactions to the contract, report or enquire on it, maintain it, and so on. The contract will not appear on their lookups, and if they enter the contract code, COINS issues a message informing them that they are not allowed to access the contract.



10.1 Configuration

Access is governed by the control field, which can be the contract code, one of the other validated fields, such as contract location, or any one of the four analysis sets.

Two Contract Status Parameters control how Contract Security will be implemented:

10.1.1 JC/JOBSEC

Which field COINS uses to control contract security.

When determining whether to allow a user access to a contract, COINS checks the value of the field specified here against the settings for that user in Contract Security Maintenance.

Enter one of the following:

- job_num for contract code
- jgr_group for contract group code
- jty_type for contract type code
- jcl_loc for contract location code
- job_fore for contract manager
- rcm_num for customer
- job_anal1 for analysis set 1
- job_anal2 for analysis set 2, etc.
- or leave blank for no contract security.

10.1.2 JC/COSECDEF

Whether a missing record in in Contract Status > Setup > Setup Maintenance > Security > Contract Security means 'None' or 'All'.

- Y = If there is no record for the user in Contract Status > Setup > Setup Maintenance > Security > Contract Security, the user has access to no contracts.
- N = If there is no record for the user in Contract Status > Setup > Setup Maintenance > Security > Contract Security, the user has access to all contracts.

10.2 Application

The following example assumes that contract security is defined by Manager Code (Job_fore)

- From Contract Status Ledger select Setup > Setup Maintenance > Security > Contract Security.
- Enter a comma separated list of all the contracts the user can access in Security List field.

[illegible]

10.2.1 Setting Contract Security by Code

In combination with, or instead of, using the control field which defines Contract Security, you can also impose security by Contract Code on a record by record basis.

In the code field, enter a can-do list of record codes that allow you to grant or deny the selected user access on a record-by-record basis when entering transactions. Blank allows access to all records

[illegible]