
PO System Security & Setup

A Guide to Usage

By Court Developers

© 2010 Court Developers.

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of Court Developers.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by Court Developers, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

Court Developers reserves the right to change details in this publication without notice.

Windows is a trademark and Microsoft, MS-DOS, and Windows NT are registered trademarks of Microsoft Corporation. Other product and company names herein may be the trademarks of their respective owners.

Table of Contents

System Security

Introduction.....	4
The Admin Section	4
Menu bar.....	4
Creating a User	6
Identification	7
Login.....	7
Name	7
Password.....	8
Additional Information	8
Menu Control.....	9
Passwords Form	10
Password Setup.....	11
Menu Permissions Group.....	12
Menu Permissions Dialog	14
Copy Permissions Dialog	15
Audit Trail	16
Audit Trail Table	18
Audit Trail Management.....	18
Users Login	19
New Password	19
Admin Tools	20
Directories	21
Environment.....	21
System Setup	21
Company Details	21
PO Print Options	22
Numbering	22
Email Setup	22
Registration Info	23
Reindex/Pack Tables	23



System Security

Introduction

The PO Large Office System has two levels of security in the application

- User Security – determining who can login and what privileges they then have;
- Form and Menu Security – controlling what forms a user can access;

User's security details are stored in an encrypted file.

Within user security there is another security control that applies only to the Admin section. This allows, for example, a manager to control the users who are a lower level than his level but prevents him accessing any settings for users with a higher access level like the system administrator.

The default admin login is

User: admin

Password: 123456

The Admin Section

Accessible from the menu bar the Admin section has all the functions that control the system setup and users.

When you select many of the security forms you'll notice a new menu bar pops up.

Menu bar



This menu bar allows you to control the security forms. Not all the buttons will be enabled on the security forms.

The button functions are;



Parent Mode – On/Off

Used to control record movement when there are child records and their parent records all on one form. (Not



used in the admin section.)

**Search**

Brings up a search form for finding records.

**Locate**

A more advanced search.

**List**

Brings up a quick selection of all records.

**Filter**

Allows complex filtering of records.

**Order**

Selects the order in which records are shown.

**Reports**

Opens the report manager.

**First**

Goes to the first record.

**Prev**

Goes to the previous record.

**Next**

Goes to the next record.

**Last**

Goes to the last record

**New**

Creates a new empty record.

**Copy**

Copies the current record into a new record.

**Delete**

Deletes the current record.

**Group Delete**

Allows multiple records to be deleted at one time.

**More**

Saves the current record and opens a new blank record.

**Save**

Saves the current record.

**Cancel**

Cancels any data added before a Save.

**Close**

Closes the form.



Creating a User

The system is supplied with a system administrator already setup with full access and privileges.

It is vitally important that you always have at least one user with these privileges or you could find yourself locked out of the system and unable to access some functions.

If there is to be only one system administrator we would recommend that a second login with full rights is created to act as a standby in case the main admin account is accidentally altered.

To create a new user first select the Users form from the Admin>Security menu. You'll then see

The screenshot shows a web form titled "Users" with the following sections and fields:

- Identification:** Login Name (User ID) [michael.smith], Staff Number []
- Name:** First [Michael], Middle [], Last [Smith]
- Additional Information:** User Email [michael.smith@courtdevelopers.co.uk], User Level (radio buttons: Director, Manager, User), Spend Limit [100000]
- Administrator:** Make this user a system administrator
- Login:** Currently Logged in?, Allow Multiple Logins
- Password:** Temporary [michael], Last Change [/ /], Period (days) [0]
- Menu Control:** Group [ADM], or blank the above box and, [Set Menus for this Individual...], Admin Access Level [A]
- Finance:** Make this user a finance operative

Click the New button on the toolbar and enter a new user's information in the fields shown. The fields on the Users form are described below.



Identification

- **Login Name:** A 20 character field which identifies the user to the application. You enter your Login Name on the Login dialog when you run the application.
- **Staff Number:** A 20 character field used to identify the user in the organization. (optional)

Login

- **Login Status:** Will be checked if the user is currently logged into the Application.

Tip: If a user is logged-in when the application is abnormally terminated due to a power failure, rebooting, etc., the contents of this field may be incorrect. If the user has not been given Multiple Login rights as described below, the user will not be allowed to re-enter the application. In this case, another user will have to uncheck the user's Login Status check box so that the user can re-enter the application.

- **Multiple Login:** If checked, the user can login to the application from more than one computer at the same time. The user can also re-enter the application if it terminates abnormally as described above. If unchecked, the user can only login if the Login Status field is unchecked.

Multiple Login Tip: At least one user should be given this right so that all users would not be locked out of the application if there is a power failure, etc.

Name

First Name: A 30 character field for the user's first name.

Middle Name: A 30 character field for the user's middle name. (optional)

Last Name: A 30 character field for the user's last name.



Password

Temporary Password: When a user is first added on the Users form, enter a temporary password in this field. Then, when the user enters the application for the first time, the user will be prompted to enter a new password of the user's own choosing.

Temporary Password Tip: Any time you make an entry in this field, the next entry into the application by the user will require the user to enter a new password.

- **Password Last Change Date:** This field contains the date of the last password change.

Password Last Change Date Tip: Blanking-out this field will cause the user to be required to enter a new password upon the next entry into the application

- **Password Period:** This field contains a 3-digit number that represents the number of days that, when added to the Password Last Change date, is the date on which the user must next change passwords. Use this field to enforce your password change requirements

Password Period Tip: An entry of zero means that the user can keep the same password indefinitely.

Additional Information

User Email: A 40 character field for the users email – used for the return address when emailing a PO.

User Level: A user may be assigned to one or more special levels of Director, Manager or User which can be used to control certain functions of the PO system operation (not available on all versions).

Spend Limit: The maximum a user can spend on a single PO before approval or other limitations occur (not available on all versions).

Administrator



Ticking this box will give the user full admin rights over the software which means all functions are available and no restrictions are placed on what they can do with creating/authorizing PO's.

Finance

Assigning a user to the Finance group gives them the ability to mark orders as fully complete. This was found to be a useful restriction so that only nominated users could record when an order had been fully reconciled all through the system.

Menu Control

Here you can control what a user has access to when using the system.

Group: A 3 character field used to assign the user the same menu permissions as all other members of the same group. This way, individual menu permissions do not have to be assigned to each member of the group. See Menu Permissions Group.

Tip: The system comes with two menu permissions set up. The 'ADM' selection has full access to all menus. The 'USR' selection has access restricted to the main PO screen and search only.

If you wish for a certain user to have access to a very specific set of menus then delete the entry in the Group box and click the 'Set Menus for this Individual...' button. This will launch the Menu Permissions dialog where you can assign menu permissions to the individual user (as opposed to assigning the user to a Menu Permissions Group).

If there is no entry in the Menu Permissions Group field, you can click the Menu Individual button to select menu permissions for this individual user. If there is an entry in the Menu Permissions Group field and you click the Individual button, the Menu Permissions dialog will only display the permissions assigned to the group. You may not change these assignments. The group's menu permissions may be changed through the Menu Permission Groups dialog

Admin Access Level: **This is a very important setting.**

- **Blank:** The user will not be allowed to access the Users or Passwords forms.



- **A-Z:** The user can access the Users or Passwords forms, but the user will only be able to view users whose Access Level is blank or less than or equal to her own Access Level. Level A is the highest and Z is the lowest Access Level. A user cannot assign an Access Level higher than her own.

Thus a manager might be assigned level 'M' and could view and alter passwords and details for all users with a designation of 'N' and lower but could not view or alter the details of 'L' or higher.

It is important that the administrator/s keep their level set at 'A'.

Passwords Form

You access the User Passwords form from the Passwords option on the Admin - Security menu. The User Passwords form is where you view and change user passwords as well as identify which users can access the form.

The screenshot shows a web browser window titled "Passwords". The form is divided into several sections:

- Identification:** Contains two input fields: "Number" (empty) and "ID" (PCook).
- Name:** Contains three input fields: "First" (Paul), "Middle" (empty), and "Last" (Cook).
- Password:** Contains two input fields: "Password" (123456) and "Last Change" (05/08/2008).
- Access:** A checkbox labeled "Access" which is currently unchecked.

You can't add users on the User Password form. You add users on the Users form. Passwords are maintained on a separate Passwords form for additional security.

On this form you can change

Password: A 20 character field that contains the user's current password. Any time you make an entry in this field, the next time the user enters the application, she will be required to enter this password.



Last Change: This field contains the date of the last password change. Blanking-out this field will require the user to enter a new password upon the next entry into the application.

Access: This check box provides an additional level of password security beyond that provided by Menu Security. If the Access check box is checked, the user has the right to access the Passwords form (assuming the user has been given the Menu Security permission). Once one user has a check entered in this field, only those users with a check can access the Passwords form. As long as all users have the Access field unchecked, any user that has been given the Menu Security permission to access the Passwords form can have access.

Password Setup

The Password Setup form on the Admin - Security menu is where you define the rules for entering new passwords.

The screenshot shows the 'Password Setup' dialog box. It has a title bar with the text 'Password Setup' and standard window controls (minimize, maximize, close). The dialog is divided into two main sections. The first section, titled 'New Password', contains several settings: 'Warning Days' is a spin box set to 1; 'Change Character' is a text box containing a question mark; 'Minimum Length' is a spin box set to 1; 'Maximum Length' is a spin box set to 10; 'Password No ID' is a checked checkbox; and 'Prior Passwords' is a spin box set to 1. The second section, titled 'Case Sensitivity', contains two checked checkboxes: 'Case-Sensitive User ID' and 'Case-Sensitive Password'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

The settings are

Warning Days: The number of days prior to the password expiration date that a warning dialog will be displayed. The warning shows the expiration date and allows a user to change passwords immediately.



Change Character: Holds the character that that when appended to the password on the Login dialog, signifies that the user wants to enter a new password. The default Change Character is a question mark, "?".

Password No ID: Check this box to prevent users from putting their Login Name in their password.

Minimum Length: A number from 1 to 20 that represents the least number of characters that can make up a password.

Maximum Length: A number from 1 to 20 that represents the greatest number of characters that can make up a password.

Prior Passwords: A number that represents how many prior passwords will be checked to prevent duplicate entry. An entry of one means that the user's current password cannot be reused. An entry of five means that the user's current and four immediately preceding passwords cannot be reused.

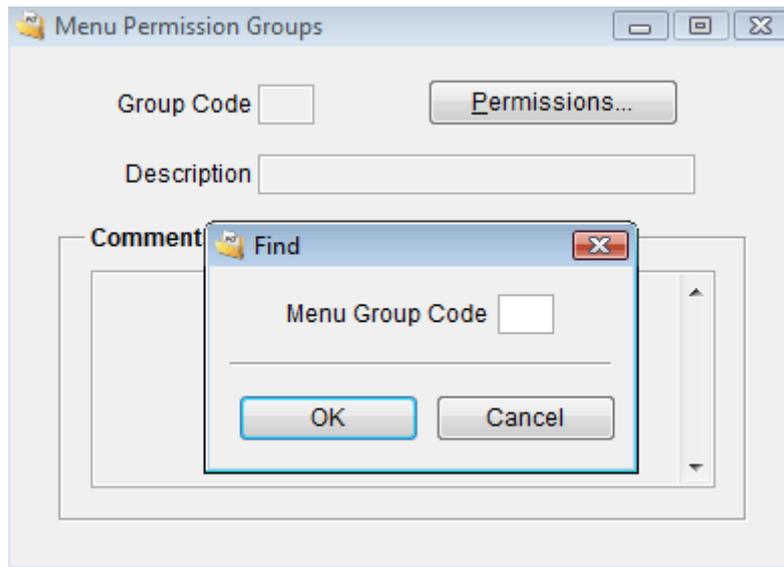
Case-Sensitive User ID: Check this box to enforce case-sensitivity when a Login Name is entered on the Security Login form.

Case-Sensitive Password: Check this box to enforce case-sensitivity when a Password is entered on the Security Login form.

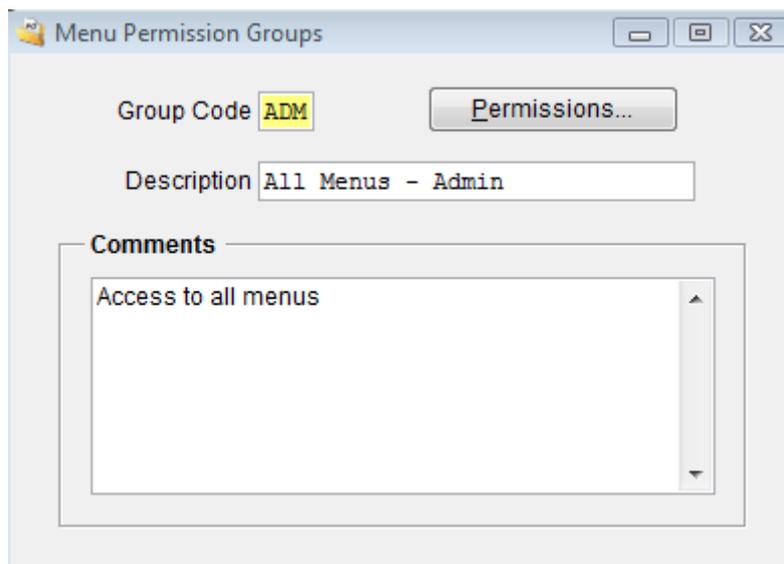
Menu Permissions Group

If a group of users will have the same permissions, you can create a menu permissions group and assign permissions to the group. Then, users can simply be assigned to this group instead of having to assign permissions to users individually.

You reach the Menu Permission Groups dialog from the Admin - Security menu.



If you want to find a specific Menu Permission Group, enter the Menu Group code in the Find form and click OK. Otherwise, click OK and the first Menu Permission Group record in order by Group Code will be displayed.



Click the New toolbar button to add a record for a new Menu Permission Group. The fields and button on the Menu Permission Groups dialog are described below.

Group Code: A three character code to identify the group.

Description: A descriptive title for the group.

Comments: A place for you to describe the group.

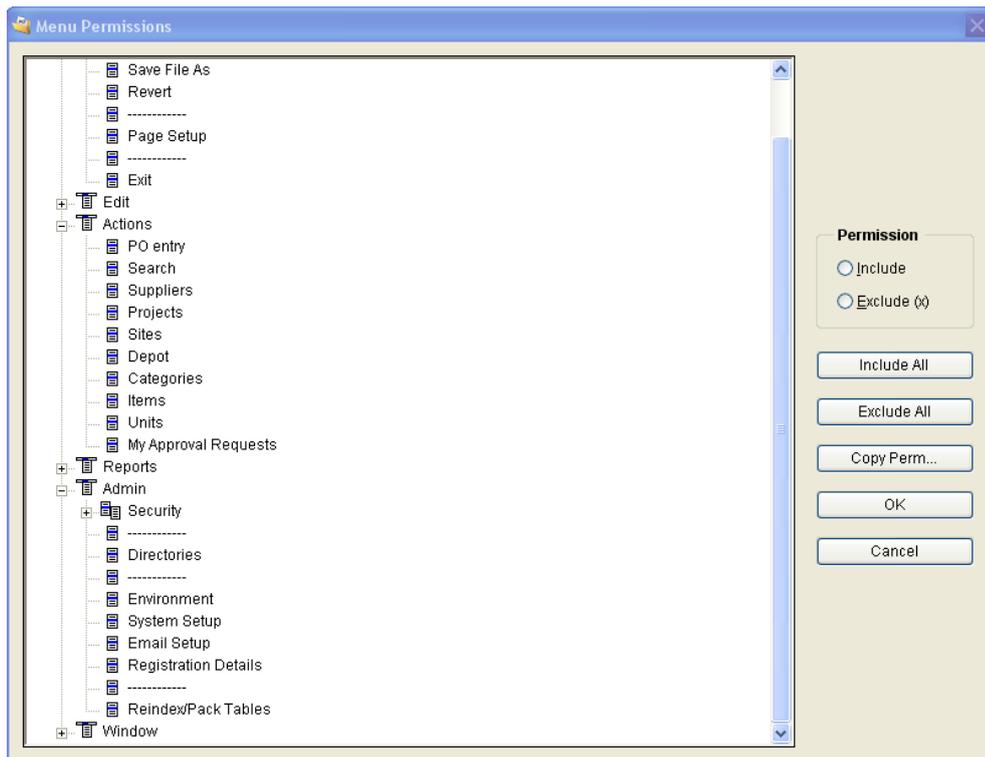
Permissions: Click the Permissions button to bring up the Menu Permissions dialog to assign permissions to the group. See the next section.



Menu Permissions Dialog

You use the Menu Permissions dialog to assign menu permissions to individuals and groups. You can reach this dialog from:

- The Menu Individual button on the Users form when you are assigning permissions for an individual.
- The Permissions button on the Menu Permission Groups dialog when you are assigning permissions for a group.



The Menu Permissions dialog lists the systems menu files in a treeview display. Expanding a menu file node displays the submenus and menu options included in the menu.

Permission Status: To the right of each submenu and menu option is the permission status. A blank means that the option will be included in the user's menu. An "(x)" means that the option will be excluded from the user's menu. By default, all menu options are excluded when the Menu Permissions dialog is first accessed for a group or individual.



The control buttons on the Menu Permissions dialog are described below.

Include / Exclude (x): Click on the Include option button to include the highlighted menu option in the user's menu. Click on the Exclude option button to exclude the highlighted menu option from the user's menu. Double-clicking on a menu option toggles its include/exclude status.

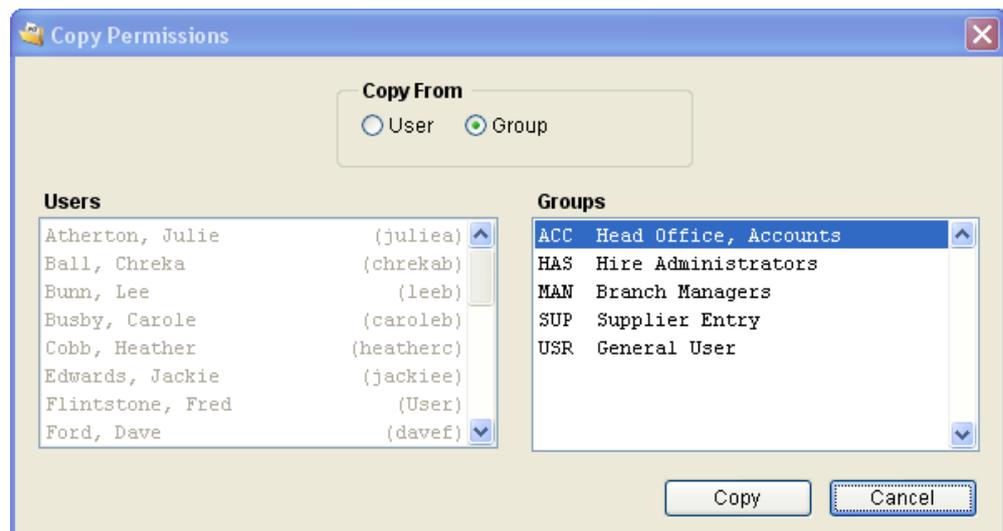
Tip: Be sure to include the File/Exit menu option so that the user has a way to exit the application.

Include All / Exclude All: Clicking the Include All or Exclude All buttons changes the status of all menu options in all menus to "included" or "excluded", respectively.

Copy Permissions: Clicking the Copy Permissions button brings up the Copy Permissions dialog where you can copy the permissions assigned to a user or group and make them the permissions of the current user or group. See the next section.

Copy Permissions Dialog

The Copy Permissions dialog allows you to assign the permissions of a selected user or group to the current user or group.



Copy From User / Group: Click on the User option button if you want to copy the permissions of a user. Click on the Group option button if you want to copy the permissions of a group.



Users List: When the User option button is selected, the Users list is enabled. Highlight the user whose permissions you want to copy.

Groups List: When the Group option button is selected, the Groups list is enabled. Highlight the group whose permissions you want to copy.

Copy: Click Copy to copy the selected permissions to the Menu Permissions dialog.

Audit Trail

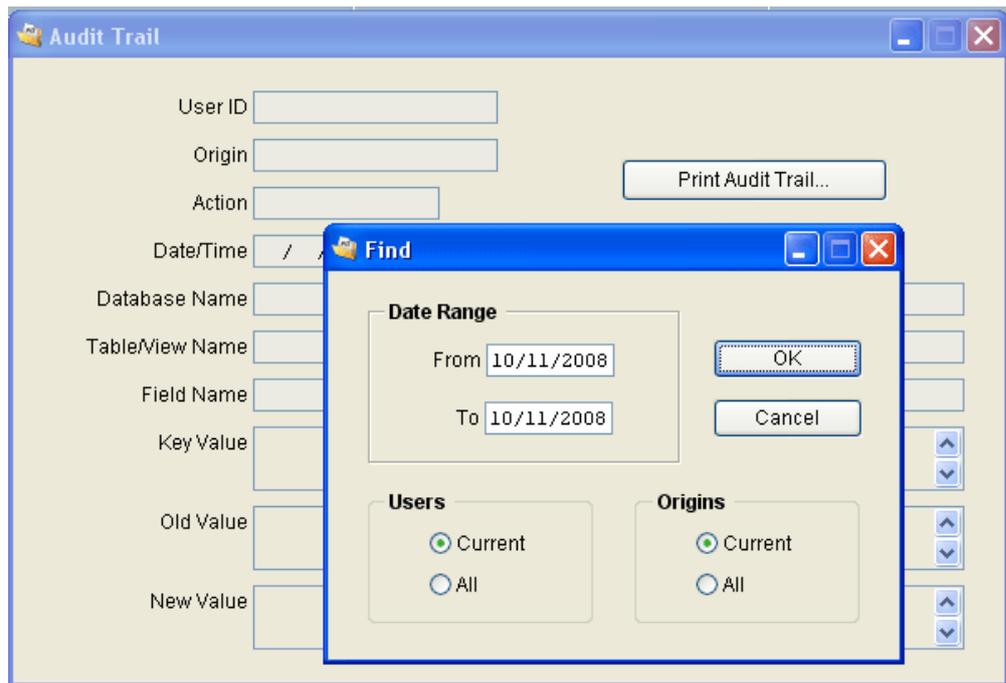
The Audit Trail records activity when data is changed or new records are added or deleted. Which areas the audit trail monitors varies according to each customer's needs and is setup by Court Developers.

The audit trail dialog box first appears with a Find box which allows selection of the audit trail records.

On the Find form, you can select:

- Date Range: Enter a date range of records to select.
- Users - You can view records for all users who have run the application by clicking the All option button in the Users box.
- Origins - All: If the application is sharing its audit trail file with another application, you can view records for all applications by clicking the All option button in the Origins box. (Not used by the majority of Purchase Order systems.)

•



Once selection has been made if there is more than one record in the results then a list of those records is shown.

The screenshot shows the 'List' application window displaying a table of audit records. The table has the following columns: Date/Time, Action, User ID, Key Value, Field, and Old/New Values. The data is as follows:

Date/Time	Action	User ID	Key Value	Field	Old/New Values
22/10/2008 02:13:02 PM	CHANGE	admin	1006	DCPOPO.PROJ_ID	103/102
31/10/2008 12:08:18 PM	CHANGE	admin	8897	DCPOPI.ITEMREC_DATE	2008-10-13/ - -
05/11/2008 02:14:45 PM	CHANGE	admin	1006	DCPOPO.LOCKED	fl
05/11/2008 03:52:01 PM	CHANGE	admin	1006	DCPOPO.ISSUED	fl
05/11/2008 03:52:01 PM	CHANGE	admin	1006	DCPOPO.LOCKED	fl
05/11/2008 03:52:03 PM	CHANGE	admin	1006	DCPOPO.ISSUED	fl
05/11/2008 03:52:03 PM	CHANGE	admin	1006	DCPOPO.LOCKED	fl
05/11/2008 03:52:11 PM	CHANGE	admin	1006	DCPOPO.ISSUED	fl
05/11/2008 03:52:11 PM	CHANGE	admin	1006	DCPOPO.LOCKED	fl
05/11/2008 03:52:13 PM	CHANGE	admin	1006	DCPOPO.ISSUED	fl

Double clicking on a record will then show that audit record in detail.



The screenshot shows a window titled "Audit Trail" with a blue title bar and standard Windows window controls. The window contains several input fields and a button:

- User ID: admin
- Origin: CPO
- Action: NEW
- Date/Time: 08/11/2006 03:05:20 PM
- Database Name: PURORDERS
- Table/View Name: DCPOSITE.DBF
- Field Name: NAME
- Key Value: 51 (with up/down arrows)
- Old Value: (empty) (with up/down arrows)
- New Value: Delivery Site 1 (with up/down arrows)

A button labeled "Print Audit Trail..." is located to the right of the Origin field.

The audit trail records information from a 'low-level' of the purchase orders data tables and shows some internal data names and information that is normally hidden from the end user. Although the names are fairly obvious if you need any specific help in identifying what a record means then just contact us.

The audit trial records can also be searched, navigated, listed by using the menu bar buttons at the top of the screen.

Audit Trail Table

The audit trial records are stored in the SDATAAudit.DBF table.

Audit Trail Management

If an application gets a lot of use, the number of records in the audit trail table can get large very quickly. Periodically, backup the audit trail table and delete its records. You can use the Group Delete Toolbar control.



Users Login

When you run the application you are prompted for a login



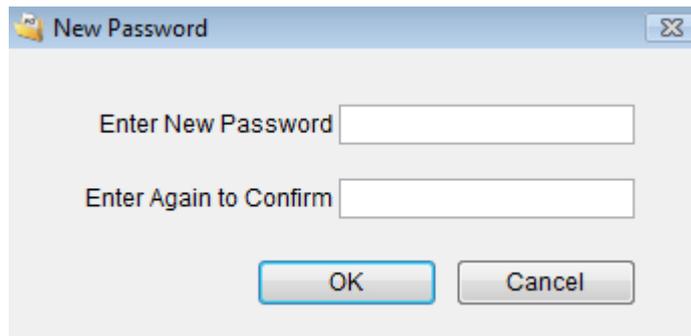
Enter your ID and password. If you press the escape key, you will exit the application. You are allowed three attempts to enter a valid password. Upon the third invalid entry, you exit the application.

Temporary Password: When you enter a new user on the Users form, you enter a temporary password for the user. When the user enters the PO system for the first time, the user will be prompted to enter a new password of the user's own choosing. The purpose of this feature is to allow only the user to know her password after the administrator assigns a temporary password.

Changing Your Password: You may enter a new password at any time by entering the "Change Character" after your password. The Change Character is a question mark, "?", but you can make it another character. The Change Character is described in "Password Setup"

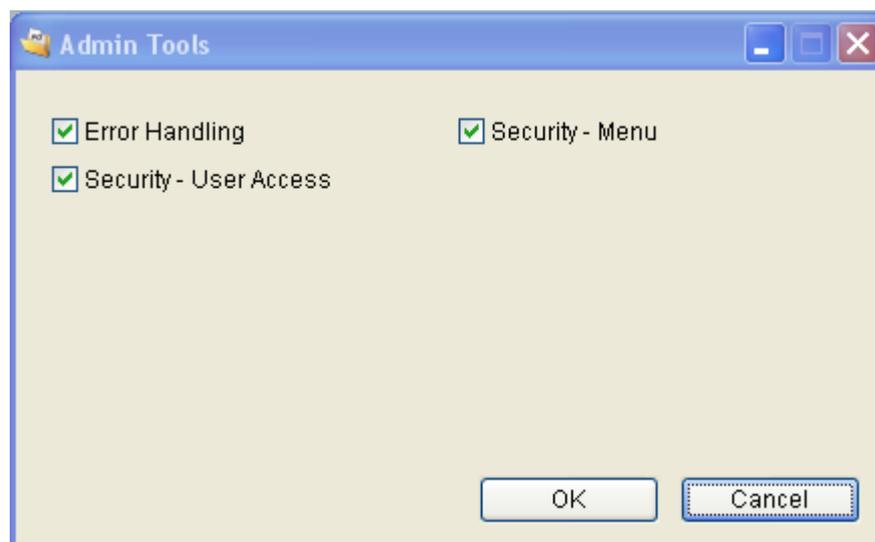
New Password

The New Password dialog requires you to enter a new password that conforms to the rules entered on the Password Setup form.



After you enter a valid password, you must enter it again to confirm your entry. This is necessary because the entries are hidden from view and you may have entered something other than what you had intended. If you decide to not enter a new password, pressing the escape key or clicking Cancel will exit the application.

Admin Tools



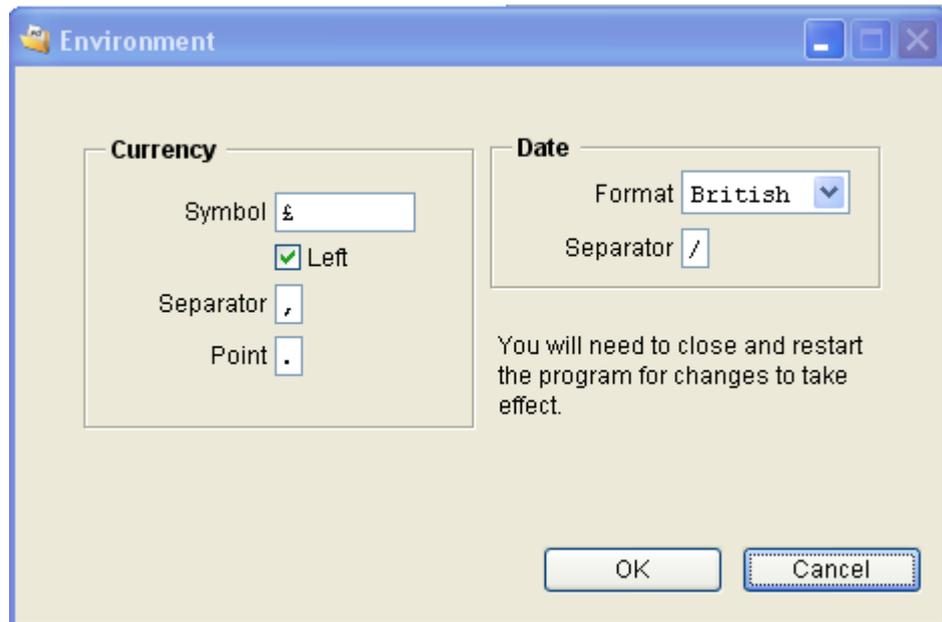
This menu item is used to enable/disable error handling which gives a more user friendly response in case of errors. It also allows the security features to be turned off for recovery purposes. These should only be used in consultation with Court Developers as disabling them will cause errors in the normal operation.



Directories

This menu item is used in some very rare network setups – do not alter unless advised by Court Developers.

Environment



Used to control regional specific settings.

System Setup

Here you enter and control the basic setup and operation of the PO system.

Most of these settings are for the demonstration version only as most customers choose to have a customized layout for the printed output which supersedes many of these settings.

Company Details

This section is used for the details that are printed out on the PO. Depending upon how much information has been 'hard-coded' into the templates for a specific customer, not all of these options may be available.



PO Print Options

Text Printed at bottom of PO: Used to insert your own text at the bottom of a PO. For example, this could be about your standard terms or specifications.

Printed Prefix: You can add a 3 character prefix to be printed out before the PO number. So if you entered 'BBC' here then PO number 2300 would be printed out as BBC2300.

Print Categories and Items: Some users like to set their systems so that as well as the item description they print out the Category and Item descriptions as well.

Show Header Image: If ticked then a header image is inserted to the top of the printed PO. This image can only be called rpthed.jpg or rpthed.gif or rpthed.bmp and must be stored in the 'pictures' folder which is found under 'Court Developers\Purchase Orders 2\' on your shared folder on the server.

You must select the appropriate extension to match the type of file you are using.

The image must be made to be 660 x 120 pixels in size – any other size will result in clipped or oddly sized displays.

Numbering

Allows you to change the PO numbering sequence.

Email Setup

Most installations only require the setting of the Outgoing mail server for email to work. Your IT department will be able to tell you this setting which may be a name like 'server1' or an IP address like 10.0.0.2.

The port number and server timeout are usually best left on the default settings unless you have a good reason to alter them.

The default subject is what appears as the subject line of your email and the default message the body of the email. You can alter these when you email a PO.



Note: Each workstation that runs the PO system will need to send mail out to the server on port 25. Some firewalls and antivirus systems may block this by default and should be checked if you have difficulty in getting email to work. The email system is entirely self-contained in the PO system and does not require any other programs to be present on the user's PC.

Registration Info

Used to enter your license registration details that will be supplied with your program.

Each workstation that accesses the PO system will need to have the license key entered into it.

Reindex/Pack Tables

This is a utility screen which performs operations on the data tables that power the PO system. We recommend you do not use this utility unless you have consulted with Court Developers first.