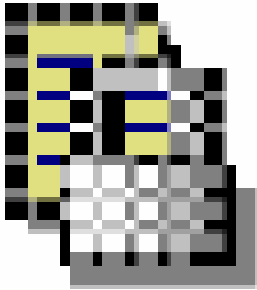


axiUm©

PowerAdmin©



User's Manual

The information contained in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exan Academic Software Inc.

© 1999-2006 Exan Academic Software Inc.

Table of Contents

1 INTRODUCTION.....	3
1.1 INSTALLING POWERADMIN	3
1.2 RUNNING POWERADMIN.....	3
1.3 THE MAIN WINDOW.....	4
1.4 CHANGE THE POWERADMIN PASSWORD.....	4
2 SECURITY LEVELS	4
2.1 ADD A SECURITY LEVEL	4
2.2 DELETE A SECURITY LEVEL.....	5
2.3 MODIFY A SECURITY LEVEL.....	5
2.4 COPY A SECURITY LEVEL.....	5
3 SECURITY RIGHTS / PERMISSIONS	6
3.1 MODIFY THE SECURITY RIGHTS.....	6
3.1.1 DIALOG BOXES	6
3.1.2 INFO MANAGER	7
Tables.....	7
Reports.....	8
3.1.3 MENU ITEMS	8
4 USERS	8
4.1 ADDING A USER	8
4.2 DELETE A USER	9
4.3 MODIFY A USER	9
4.4 MOVE A USER TO A DIFFERENT SECURITY LEVEL.....	9
5 Export.....	10
5.1 Security Level Export.....	10
6 Find Dialog	11

1 INTRODUCTION

axiUm's security is administrated by PowerAdmin. PowerAdmin is a separate application from axiUm, installed independently on selected administrator workstations. It is intended only for use by Administrative personnel to set up users, security levels and their rights for axiUm.

axiUm application users can be added to the system from PowerAdmin and assigned to a security level, or can be added within the axiUm application. Each security level consists of a set of rights and privileges for the axiUm program. Before being able to fully implement axiUm, PowerAdmin must be used to set up security levels, users, and security rights for all personnel that will operate the axiUm Clinic Management System.

1.1 INSTALLING POWERADMIN

The PowerAdmin application consists of a single executable file - "**PowerAdm.exe**"

Install PowerAdmin on a station that already has axiUm installed. The PowerAdmin executable file must be copied into the axiUm directory on the station's hard drive. A shortcut to the application can then be created. If the station does not already have axiUm installed, then the user should refer to the instructions for setting up a client station for axiUm, as there are many steps involved before PowerAdmin will function.

There must be some consideration given to the location of station(s) installed with PowerAdmin as it has utmost importance on the integrity of axiUm. Even though access to it is password protected, PowerAdmin should only be installed on stations within closed offices where access and use is restricted.



Warning! If a version warning message is displayed, obtain the correct version from your IT department or Axium Support before proceeding.

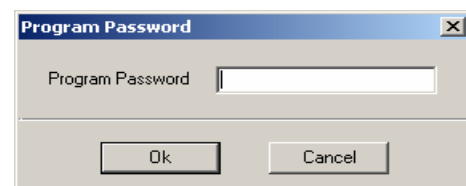


1.2 RUNNING POWERADMIN

If the PowerAdmin shortcut icon has been placed on the desktop, all the user has to do to begin the program is double click on the PowerAdmin icon or open "PowerAdm.exe" from the directory it is installed on with Windows.

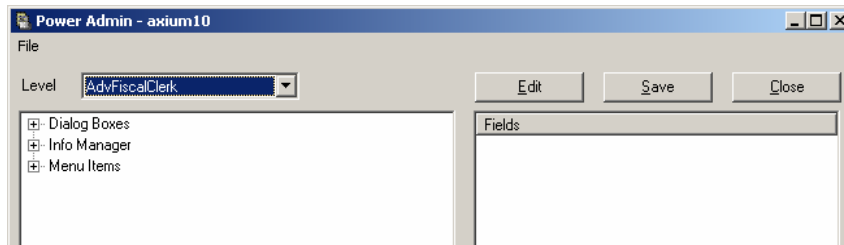
The "**Program Password**" dialog box will appear prompting the user to enter the application password for PowerAdmin.

This password is station specific, so that each station installed with PowerAdmin may have a unique password. This password may be changed once the application is running (See section 1.4).



For first time use, the default password is "**poweradmpass**". This is the default password for any installation of PowerAdmin. It should be changed immediately upon accessing the program.

The password is case-sensitive, and an invalid entry will simply close the dialog. Entry of the valid password will open the PowerAdmin application's main window.



1.3 THE MAIN WINDOW

PowerAdmin's main window consists of a single pull down **File** menu in the upper left that provides access to the setup of security levels (see Section 2) and creation of users (see Section 4). The main window has two areas for the setup of axiUm security rights and for the setting of permissions for security levels (For details see Section 3).

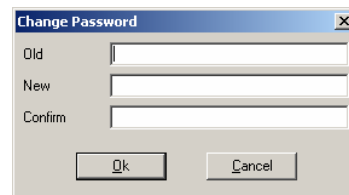
Remember! The **Close** button closes PowerAdmin, not just the current dialog.

To exit PowerAdmin, click the **Close** button in the upper right corner of the window. If you have not saved your changes the system will prompt you to do so before the close is performed.

1.4 CHANGE THE POWERADMIN PASSWORD

To change the PowerAdmin password select "**Password**" from the "**File**" drop-down menu to display the "Change Password" window.

Type in the old program password (for new installations this will be "poweradmpass"), the new password, and confirm the new password before pressing the Ok button to complete the password change.



Note: The **Encrypt Passwords** menu item will encrypt all of the passwords stored in Axiom and has no effect on the PowerAdmin password.

2 SECURITY LEVELS

Each axiUm security level defines the rights and permissions of a set of users in axiUm. A security level can have any name and the name should represent the user group function. Examples of typical names for security levels are Administrator, Instructor, Student and Cashier. For each security level, appropriate access rights can be granted (See section 3.1). Individual users are assigned to a security level, giving each axiUm access rights as specified for their particular level.

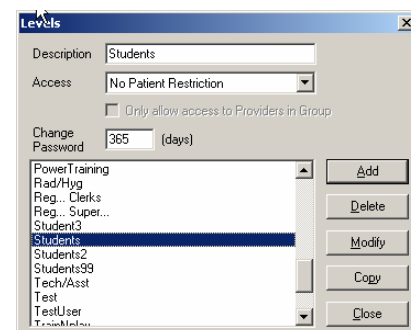
Selecting **Levels...** from the **File** drop-down menu will display the Security Levels dialog.

2.1 ADD A SECURITY LEVEL

Enter a Description for the new security level.

From the **Access** drop-down list, select the appropriate access option for the level to be added:

Administrator - full access to patients and providers in the axiUm system. Specific restrictions can not be set for this access level and any changes will not be saved. This option should only be selected for an Administrator level that will consist of a very limited set of administrative and technical personnel. When a level of this access type is selected a warning comes up.



No Patient Restriction - allows users of the level to view and access all patients in the active database.

This type of access is for non-restricted levels.

Restrict to Assigned Patients - limits users of the level to view and access only those patients that they are assigned to as the patient's provider. This option is typically selected for student levels.

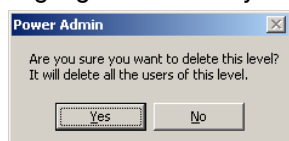
Only Allow Access to Providers in Group - This checkbox is to restrict student levels to a particular group. Limits users of the level to view and access only those providers in his provider group such as GP1. This option is grayed out for non-restricted levels.

Change Password - For security, a user level can be forced to change passwords after a certain number of days. If no forced password changes are in effect this should be set to 0.

Click on the **Add** button to add the new level to the list of security levels.

2.2 DELETE A SECURITY LEVEL

Highlight the security level to delete by left clicking on the level in the list.



Click on the **Delete** button. The program will display a warning box as shown here to verify that deleting the security level will also delete any users assigned to the level and all of the work done in setting the level permissions will be lost. For these reasons it is very important to be certain that the level is no longer of use and the users of a security level to be deleted have already been moved to a different level before actually deleting the level (See section 4.4).

Select **Yes** to delete the level and all users of the level or select No to cancel the delete command.

2.3 MODIFY A SECURITY LEVEL

Select the security level to modify by left clicking on the level in the list. The entry cells will display the information for the selected level.

Make the necessary modifications and when finished making changes, click on the **Modify** button. If the Access Level has been modified, the program will prompt the user to confirm the change before continuing if the access setting has changed.

Note: To edit the security rights for a selected level see section 3.

2.4 COPY A SECURITY LEVEL

Copying a security level is very useful when another security level is needed that is very similar in access rights to an existing level that has already been setup. Select the security level to copy by left clicking on the level in the list.

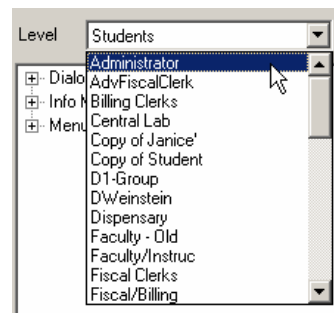
Click on the **Copy** button. This will add a new security level, with a description beginning with "Copy of " followed by the description name (possibly clipped to fit) of the level that was copied. This description can be modified as required and the changes saved with the **Modify** button.

This new level will have all the security rights as assigned to the level that it was copied from. To make modifications to these privileges see section 3.

3 SECURITY RIGHTS / PERMISSIONS

For each security level created, a set of axiUm access rights must be assigned. When setting up axiUm security rights it is easiest to think of it as removing unneeded privileges from certain levels. For example: A student level does not require access to printing receipts, making payment adjustments, setting grades or accessing accounts receivable. In a similar fashion the front office accounting staff does not require access to periodontal charts or grading information.

The PowerAdmin main window is used for the setup of security rights. When working in the main window, select the security level to work with from the Level drop-down list in the upper left of the window.



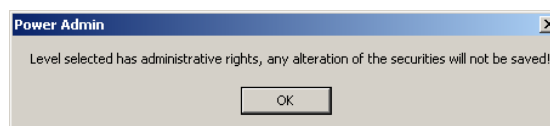
To save some time in the setup, it is recommended that the ability to copy levels be used when setting up security levels with similar permissions (see "Copy a Security Level").

Note: To save the changes you must click the Save button.

3.1 MODIFY THE SECURITY RIGHTS

Select the security level to modify from the Level drop-down list. If the level has administrative security rights the access can not be altered.

Once a level has been selected this will refresh the lower left list to display 3 lines: **Dialog Boxes**, **Info Manager**, and **Menu Items**. Each line can be expanded to display more detail for the selection. For information for the items listed refer to the following sub-sections.

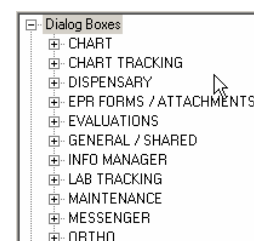


When finished making changes click on the **Save** button to write the changes to the database. To cancel your changes select a different security level from the Level drop-down list, or click the Close button to exit PowerAdmin. The message "Changes will be lost, Continue?" will come up. To lose the changes select "Yes", to close the message and save changes click "No".

3.1.1 DIALOG BOXES

Dialog boxes are a software term used to describe the various windows and screens that make up the program. There are many dialog boxes in the axiUm program and each may be set up with distinct security rights.

Note: To disable access to an entire module select **Main Program** from the list and unselect the checkbox beside the module name. This step eliminates the detailed selection of access to individual dialogs (see Section 3.1.1) for a "restricted" module.



To view the list of dialogs, expand the **Dialog Boxes** line item by clicking on the plus sign (+). The list of dialogs will now appear. The list is long but is broken into sections based on the module that the dialog is accessed from.

To view/modify the security rights for a specific dialog, **double-click** on the dialog's line in the list or select the dialog and click the **Edit** button. Alternatively, you may single-click on the line to select it, and then click the Edit button. This will open the PowerAdmin permission view of the dialog.

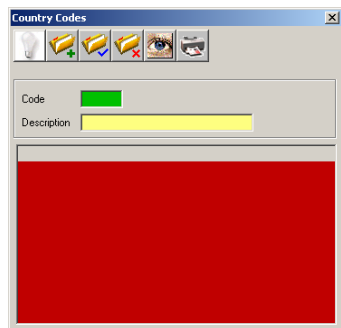
The dialog will appear the same as it appears in axiUm, with a few modifications: Edit fields will appear in color, buttons may also be in color or, in some cases, grayed out.

The dialog security works as follows:

For buttons or icons, there are two possible security statuses: Available to the user and Restricted from the user. When **buttons** are shown in **Green** or in their natural state they are Available to the user level. Buttons that are **Red** or **grayed** out are **restricted** from the user level. Restricted buttons will display in axiUm as grayed out. In axiUm, users are unable to click on a restricted button.

To change the security status of a button, simply left click on the button. This will alter the buttons security status and change the color of the selected button.

For edit fields and lists, there are 3 possible security statuses: **Read and Write** access (**GREEN**), **Read-only** access (**YELLOW**) and **No access** (**RED**). These 3 statuses are represented by the field or list appearing in color. To change the security status of a field or list, left click on it in the dialog. This will cycle the color of the field through the three security statuses.



To assist in setting these securities, right click anywhere in the dialog box to display a menu of security choices.

Enable All (Green): Sets all fields and buttons on the dialog box to green.
Disable All (Yellow): Sets all fields and buttons on the dialog box to yellow.
Disable All (Red): Sets all fields and buttons on the dialog box to red.
Copy Dialog Settings: Allows the user to select another security level to

copy this dialogs security to. The user can multi-select levels by holding the Ctrl key down on their keyboard while clicking on level names.

Copy Control Setting: If the user right clicked on a control field, allows the user to copy the setting for this single control to another security level.

Show Control Settings: If the user right clicked on a control field, allows the user to see each security level and it's current access rights for the field selected.

When you are finished modifying the security rights to an individual dialog, close the dialog by clicking the 'x' in the upper right corner of the dialog or by pressing the Escape button on the keyboard. Not all dialogs have a close button so you may be required to press the Escape key to exit the dialog.

Once the dialog has been closed, the main window displaying the list of dialogs will be shown again.

3.1.2 INFO MANAGER

The Info Manager is axiUm's report generator. It allows users to run over 200 standard reports and create custom reports based on most of information stored in axiUm. PowerAdmin can restrict access to certain information and to specific reports within Info Manager. When the Info Manager line is expanded in the PowerAdmin main window, two additional lines are displayed below it: **Tables** and **Reports**.

Tables

Table security allows the administrator to prevent selected user levels from viewing or reporting on specific table and data field information. To restrict a security level from reporting on certain information in the database, expand the Tables line item. This will reveal all of the axiUm data tables that are available in the Info Manager.



Select the table in the list by left clicking on it. The **Fields** associated with the selected table will then display on the right hand side of the window. To prevent access to a specific field, simply unselect the checkbox beside the field. By doing this, any user of the selected level will not be able to include the restricted field in any reports in Info Manager. For example, a researcher could be allowed to report on patient sex, age and postal code only, and may be restricted from seeing any patient names, chart numbers, phone numbers or addresses.

Reports

To restrict access to a specific Info Manager report, click on the Reports item in the list. All of the Info Manager reports will be listed on the right hand side.



To restrict a report, unselect the checkbox beside the report. With the item unchecked, the report will not appear as a selection when the user is in the Info Manager.

3.1.3 MENU ITEMS

The **Menu Items** section includes all right click menu items in the axiUm program. When the list is expanded, it displays menus found in axiUm's functional areas like the Scheduler, Rolodex and Transactions.



To edit permissions for a menu, select the axiUm module in the list. This will then display the individual menu items for that module in the Fields List box. Deselect the checkbox beside any menu item that should be disabled for the security level you are defining.

The "Main Program" list item is used to set the user level rights to all of the main modules in axiUm. If you do want this security level to have access to any of the transactions windows deselect Transactions in the right side list.

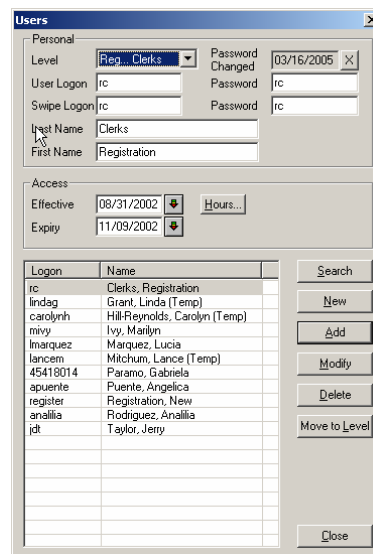
4 USERS

Users must be added for any person who will be accessing the axiUm program. This may include students, faculty, front office staff, administrators and researchers.

Users are assigned to a previously entered security level (See section 2). Each user is given a Login ID and Password to gain access to axiUm.

Throughout axiUm, records are stamped with the user that added, modified or deleted the record. This is based on the user that is currently logged into the system. Therefore, the integrity of the system relies on the security of the user Login ID's and Passwords.

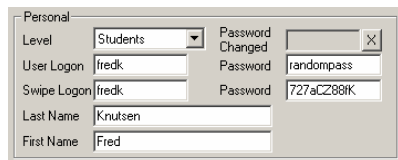
Selecting "Users..." from the "File" drop-down menu will display the Users dialog as shown here...



When working in the Users dialog, the users displayed in the lower list are the users for the security level shown in the Level field in the upper left of the dialog. To view, add, modify or delete a user, first select the security level to work with from the Level drop-down list.

4.1 ADDING A USER

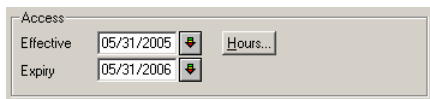
Click on the **New** button to clear the edit cells in preparation for the new entry. From the Personal area **Level** drop-down list, select the security level that the new user will be added to. If a suitable level does not exist, refer to section 2 to add a new security level.



Enter an axiUm User Logon. Each user must have a unique identification. Enter a **Password**. In axiUm the User ID and Password are both case-sensitive. The **Swipe Logon** and Password are for use with a magnetic card based system, leave these fields blank if your institution has not implemented swipe cards.

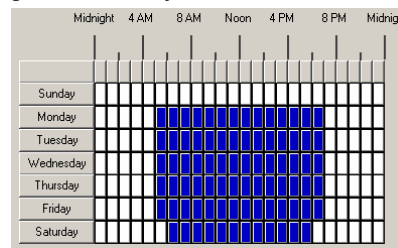
Enter the **Last Name** and **First Name** of the user as axiUm should display it.

The Access **Effective** and **Expiry Date** fields specify the axiUm access date-range for the user. Leave these fields blank to indicate no set date limitations to axiUm.



The **Hours...** button opens a dialog that allows you to restrict the times at which the selected user may access axiUm on a

daily basis. Clicking any of the one hour time boxes will blank it out or turn it blue. Blue indicates that access to axiUm is allowed. Leaving all of the boxes blue allows the user to log into axiUm at any time.



Click on the **Add** button to add the newly created user to the database. The new user will now appear in the lower list of users for the selected security level.

Note: The Effective and Expiry Dates should be set for users that are not permanently assigned to use axiUm such as students and temporary staff.

4.2 DELETE A USER

Select the user to delete by highlighting the list entry. Click on the **Delete** button. A **warning box** is then shown to verify the deletion. Select **Yes** to delete or **No** to cancel the deletion.

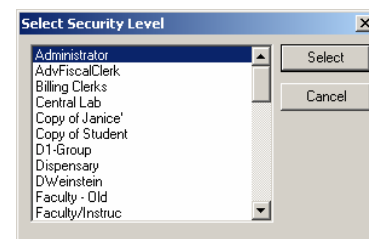
Note: Even though a user is deleted, the user may still appear in certain areas of axiUm due to auditing requirements. The user will not be allowed to enter or use axiUm in any way once they have been deleted.

4.3 MODIFY A USER

Select the user to delete by highlighting the list entry. Make modifications to the user entry. Click on the **Modify** button to update the User entry.

4.4 MOVE A USER TO A DIFFERENT SECURITY LEVEL

Often a user will to be reassigned to a different security **Level** to gain certain access privileges or have some revoked. To do this a user can be moved by PowerAdmin from one security level to another. Examples of when this may be required are: When a student goes from third year to fourth year, a part-time faculty member becomes full time or a staff member is promoted or re-assigned. If no appropriate level exists to assign to the user, then a new level must be created (**See section 2**). To reassign a User's security level:



Do not select a new Level from the User dialog drop down list. This will change the users being listed as this setting controls the users being displayed.

Select the user from the list. Click on the **"Move to Level"** button and select the security level to move the user to. Click on the **Select** button to move the user to the selected level or **Cancel** to cancel the level move. When the dialog closes and returns to the Users window the users list will no longer list the user that was moved from one security level to another. To view that user, select his/her new security level from the Level drop-down list to display the appropriate User list.

5 EXPORT

5.1 Security Level Export

The **Export** menu item allows the axiUm access settings for a level to be exported to a text file. The export file can be in a formatted plain text format or in a comma separated values (CSV) format. The plain text format is best for documentation purposes. The CSV format can also be viewed with any text editor but has the advantage of being directly loadable by spreadsheet applications like Excel where it is easy to compare user security level settings.

```
Security-For-Level--Faculty%  
%  
%  
%  
Dialogs-With-Security:%  
*****  
%  
CHART-TRACKING--Chart-In,201,Red%  
CHART-TRACKING--Chart-In,2,Red%  
CHART-TRACKING--Chart-In,101,Red%  
CHART-TRACKING--Chart-In,102,Red%  
CHART-TRACKING--Chart-In,103,Red%  
CHART-TRACKING--Chart-In,502,Red%  
CHART-TRACKING--Chart-Out,201,Red%  
CHART-TRACKING--Chart-Out,101,Red%  
CHART-TRACKING--Chart-Out,102,Red%  
CHART-TRACKING--Chart-Out,103,Red%  
CHART-TRACKING--Chart-Out,701,Red%  
CHART-TRACKING--Chart-Out,702,Red%  
CHART-TRACKING--Chart-Out,207,Red%  
CHART-TRACKING--Chart-Out,208,Red%  
CHART-TRACKING--Chart-Out,901,Red%  
CHART-TRACKING--Chart-Out,502,Red%  
CHART-TRACKING--Chart-Out,206,Red%  
CHART-TRACKING--Chart-Out,601,Red%  
CHART-TRACKING--Chart-Out,205,Red%  
CHART-TRACKING--Chart-Out,204,Red%  
CHART-TRACKING--Chart-Out,203,Red%
```

The formatted text version of the export file (see the example at left) contains the defined levels and sections for each level for Dialogs,

Info Manager Tables/Reports and Menus that have defined security.

The CSV format export file (an example is at right) lists the same information but in a spreadsheet format. Each row contains the security level number and name in the first and second fields. The next field is "D", "I", or "M" meaning that this line is a Dialog, Info Manager, or Menu item.

	A	B	C	D	E	F
1	26	Faculty	D	CHART TRACKING - Chart In	201	Red
2	26	Faculty	D	CHART TRACKING - Chart In	2	Red
3	26	Faculty	D	CHART TRACKING - Chart In	101	Red
4	26	Faculty	D	CHART TRACKING - Chart In	102	Red
5	26	Faculty	D	CHART TRACKING - Chart In	103	Red
6	26	Faculty	D	CHART TRACKING - Chart In	502	Red
7	26	Faculty	D	CHART TRACKING - Chart Out	201	Red
8	26	Faculty	D	CHART TRACKING - Chart Out	101	Red
9	26	Faculty	D	CHART TRACKING - Chart Out	102	Red
10	26	Faculty	D	CHART TRACKING - Chart Out	103	Red
11	26	Faculty	D	CHART TRACKING - Chart Out	701	Red
12	26	Faculty	D	CHART TRACKING - Chart Out	702	Red
13	26	Faculty	D	CHART TRACKING - Chart Out	207	Red
14	26	Faculty	D	CHART TRACKING - Chart Out	208	Red
15	26	Faculty	D	CHART TRACKING - Chart Out	901	Red
16	26	Faculty	D	CHART TRACKING - Chart Out	502	Red
17	26	Faculty	D	CHART TRACKING - Chart Out	206	Red
18	26	Faculty	D	CHART TRACKING - Chart Out	601	Red
19	26	Faculty	D	CHART TRACKING - Chart Out	205	Red
20	26	Faculty	D	CHART TRACKING - Chart Out	204	Red
21	26	Faculty	D	CHART TRACKING - Chart Out	203	Red
22	26	Faculty	D	CHART TRACKING - Chart Out	902	Red
23	26	Faculty	D	CHART TRACKING - Chart Out	103	Yellow
24	26	Faculty	D	CHART TRACKING - Chart Out	104	Red

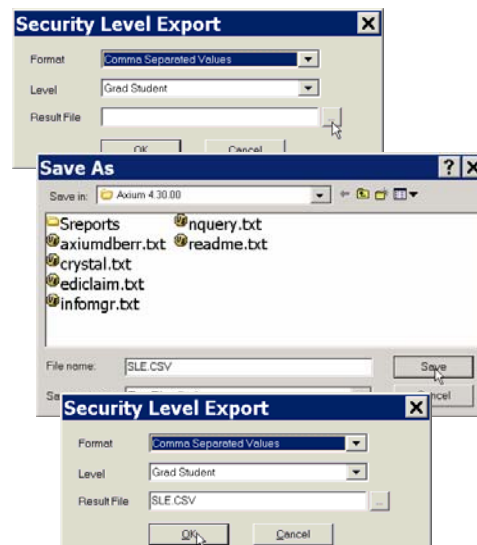
Fields 4 and 5 contain the security item name (prefixed with the AxiUm module name) and the unique internal identity for the dialog element (Info Manager and Menu items do not have these values). These values are unique for the dialog and not for the entire AxiUm program. In the above example the AxiUm "Chart Tracking" module dialogs "Chart In" and "Chart Out" both have a dialog item with the ID 201. Although the ID numbers do not tell the user that this is the dialog's "OK" button the ID code is useful in comparing user security level settings and determining if they are the same.

The last field is set to the value "Red", "Yellow" or "Green" indicating that the item is:

- "Red" - not available for use by users of this security level
- "Yellow" - visible but disabled
- "Green" - visible and usable

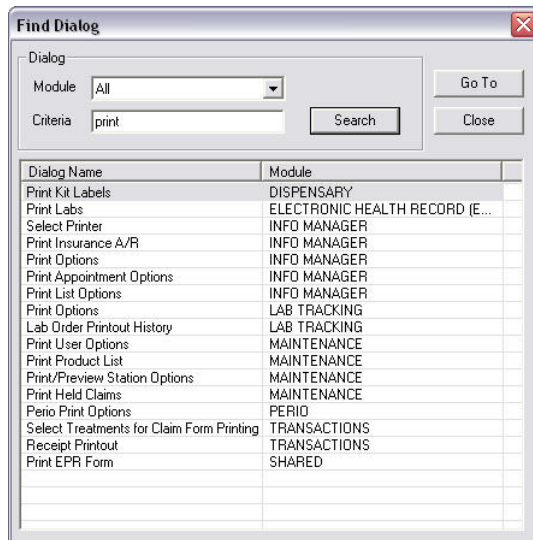
After selecting one or all security levels and the export file format save the security information in the export file by typing in the path or using the browser to select a new directory and/or an existing file name.

The default extension is ".TXT". If exporting in the CSV format it is advised to manually type a ".CSV" extension on the name so that spreadsheet applications will recognize the format.



6 FIND DIALOG

If you are having difficulty finding a dialog in the PowerAdmin lists, right click anywhere in the list window to access the “Find Dialog” window.



The Find Dialog window is a standard Windows-style dialog box. It has a title bar with the text "Find Dialog" and a close button (X). Inside, there's a section labeled "Dialog" containing a "Module" dropdown menu set to "All", a "Criteria" text box containing the word "print", a "Search" button, a "Go To" button, and a "Close" button. Below this is a table with two columns: "Dialog Name" and "Module". The table lists various dialogs and their associated modules.

Dialog Name	Module
Print Kit Labels	DISPENSARY
Print Labs	ELECTRONIC HEALTH RECORD (E...)
Select Printer	INFO MANAGER
Print Insurance A/R	INFO MANAGER
Print Options	INFO MANAGER
Print Appointment Options	INFO MANAGER
Print List Options	INFO MANAGER
Print Options	LAB TRACKING
Lab Order Printout History	LAB TRACKING
Print User Options	MAINTENANCE
Print Product List	MAINTENANCE
Print/Preview Station Options	MAINTENANCE
Print Held Claims	MAINTENANCE
Perio Print Options	PERIO
Select Treatments for Claim Form Printing	TRANSACTIONS
Receipt Printout	TRANSACTIONS
Print EPR Form	SHARED

Enter your search criteria (usually the title of the window within axiUm) and click search.

All possible results will be listed. To view the listed dialog, double click on the selection that you want. The Find dialog will auto minimize, and the selected dialog will open. Once securities are set on the dialog, or the close button is pressed, the window will refresh and display the find dialog list again.