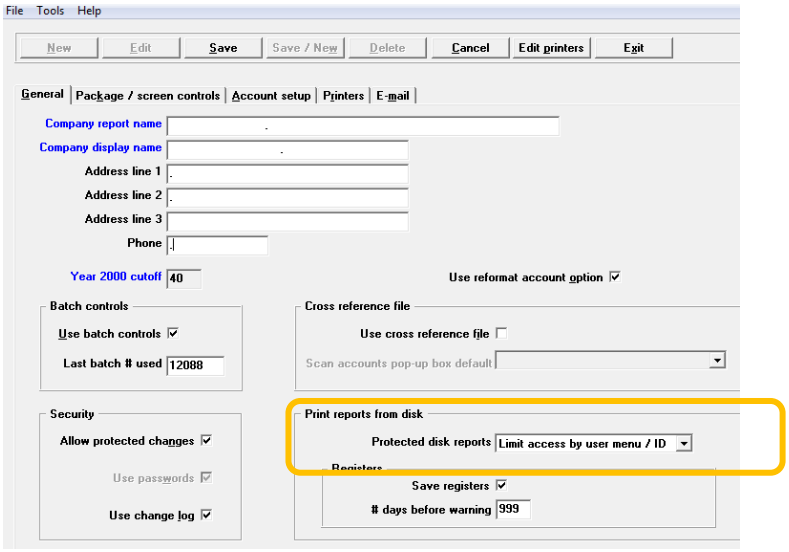
Tips &Tricks #47 – Security Options in Passport

This article continues last month's discussion of security features within the Passport accounting system. In the last installment we covered managing and control, and who could do what within the accounting system and how this is implemented by limiting menu elements available to a general user.

Report Access Protection

A related issue is posed by the question: "If a Passport user is not involved with Payroll, should they be allowed to see Payroll reports?" The same can be asked of the General Ledger and other modules that hold or generate sensitive reports and information. To answer this, Passport has a feature to restrict a user from seeing reports for a program/function they are unable to run. Since every report and function that produces a report (like a posting) has a corresponding menu entry, if they can't run the report/function because the menu entry has been removed, then Passport also ensures they can't see the output from that reporting program/function. Example - in AR, if the user does not have the ability to run the 'Reports, general/Aging' they will not be able to view any AR Agings.

Activate this function in the "CTL" menu selection in Company Information. On Tab 1 in the 'Print report from disk section', select "Limit access by user menu ID":



This is an "admin only" function and is described in the Administration Guide in the 'Company Information' chapter, under the section devoted to Tab 1. (See the previous installment for some notes on the use of the Admin manual).

Special Fields and Logging

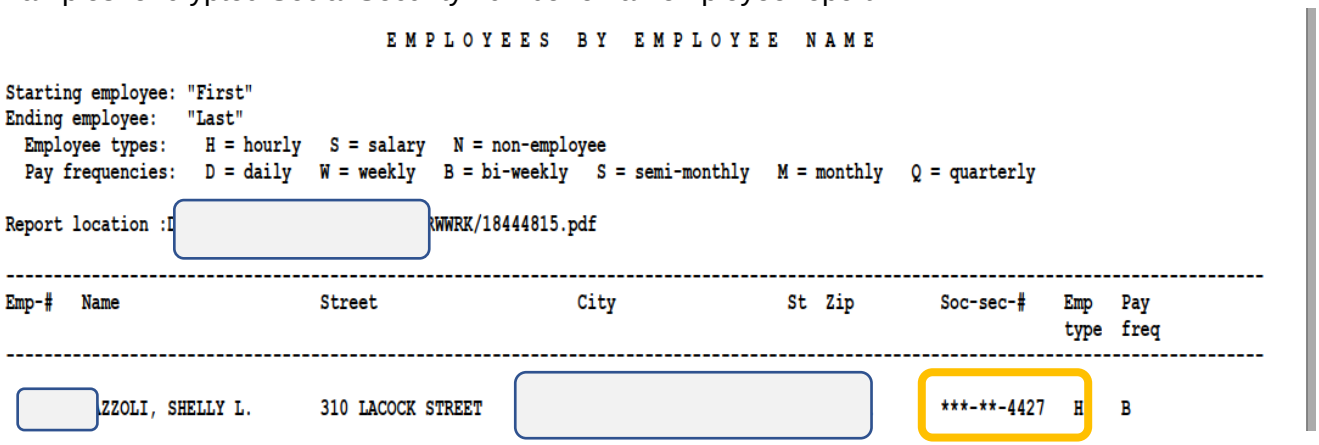
Encrypted data

In Accounts Payable and Payroll there can be very sensitive information in the form of bank account numbers used in ACH transfers – both corporate and employee – and in PR e.g., social

security numbers. Protecting access to this data from illegitimate change is done by limiting access to the maintenance functions., For example, the ACH setup functions in the Payroll direct deposit. This area was described in the previous installment.

You may also want to protect these numbers from being viewed either on an active screen, when the employee steps away from their desk, or as a field in a printed report or even after the data is exported to a text file. All three situations are handled in Passport by encrypting these data fields. That means that whenever these fields are displayed on a screen or in a report only the last four digits of the number are visible, and the remainder are replaced with asterisks. This should be familiar to anyone with online experience where, for example, your credit card number is displayed in this fashion in all cases except when you are actually in the account maintenance function maintaining credits cards.

Examples: encrypted Social Security number on an employee report:



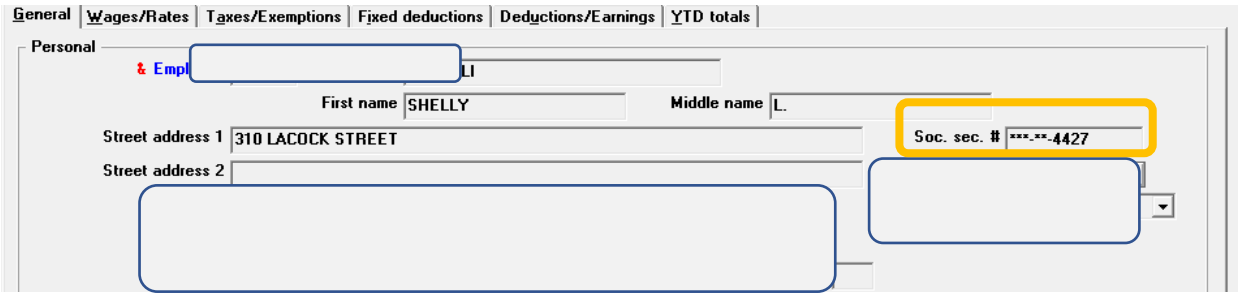
E M P L O Y E E S B Y E M P L O Y E E N A M E

Starting employee: "First"
Ending employee: "Last"
Employee types: H = hourly S = salary N = non-employee
Pay frequencies: D = daily W = weekly B = bi-weekly S = semi-monthly M = monthly Q = quarterly

Report location :D [redacted] WWRK/18444815.pdf

Emp-#	Name	Street	City	St	Zip	Soc-sec-#	Emp type	Pay freq
[redacted]	LZZOLI, SHELLY L.	310 LACOCK STREET	[redacted]			***-**-4427	H	B

and on an Employee maintenance screen:

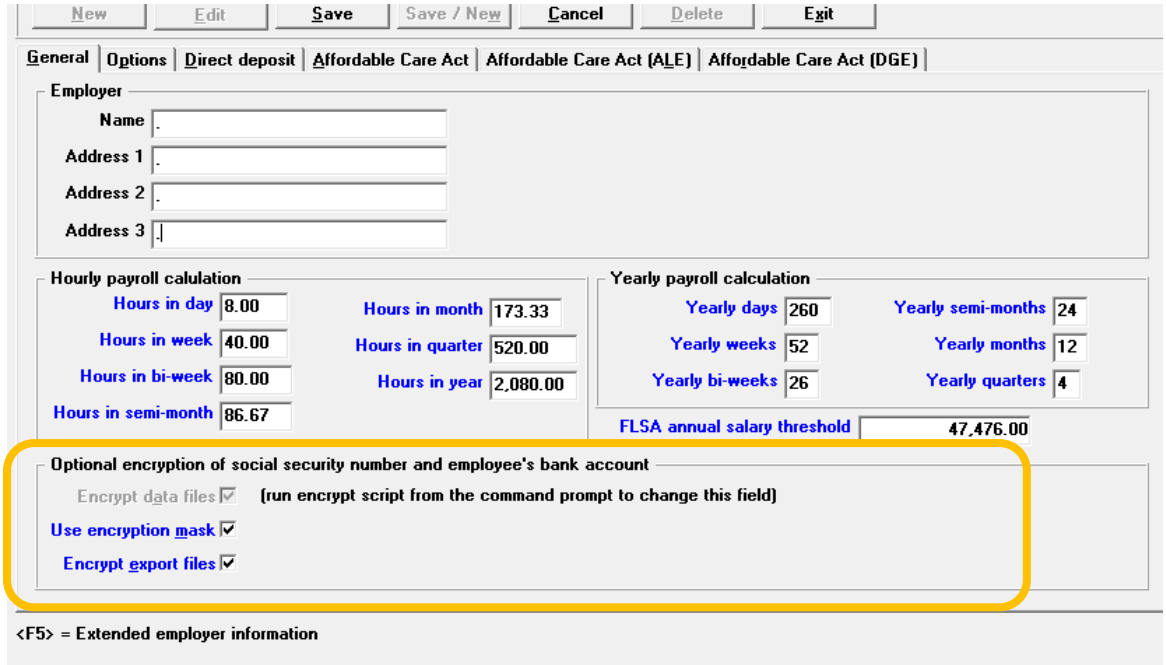


In Passport, the data is actually stored in encrypted form in the database which means that no exporting or other access to the system (e.g., a SQL or ODBC query or exporting the file with a file utility) will be able to access the unencrypted data. While the encrypted asterisk's will always be displayed at first, when you actually go into that particular field to edit it, the encryption disappears and the data is viewable until you exit the field, at which time the asterisks return.

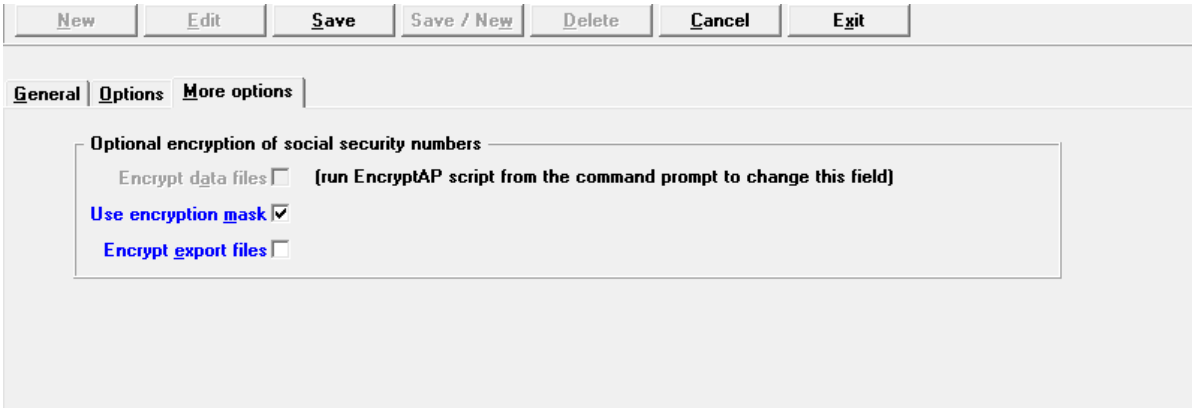
The implementation of this function is done separately in AP and PR. In each, an Encryption Utility is run to modify the fields to be encrypted. Certain other options are also available as described in the Control Information panel. Running the utility requires admin level access and, instructions for PR are located in the Control Information chapter near the end of the documentation for the first tab (search for "Optional Encryption"). For AP, this documentation is

located toward the end of the Introduction to Control Information and again search for “Optional Encryption”.

Turning this function on or off requires that you export the appropriate data file, change the option for the encryption flag in the control file entry of the module and reimport the data. For example, here is the encryption control section of the PR Control file:



Similar functionality is provided in AP for bank accounts used in ACH funds transfer. Details for adding or turning off encryption are provided in the PR and AP documentation on the ‘Master information/Control information sub-menu’ (PR – first Tab, AP – third Tab). The AP third tab of the Control Information:

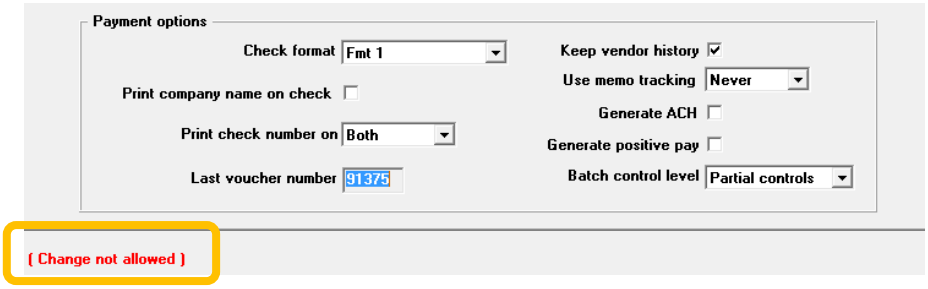


Protected Fields

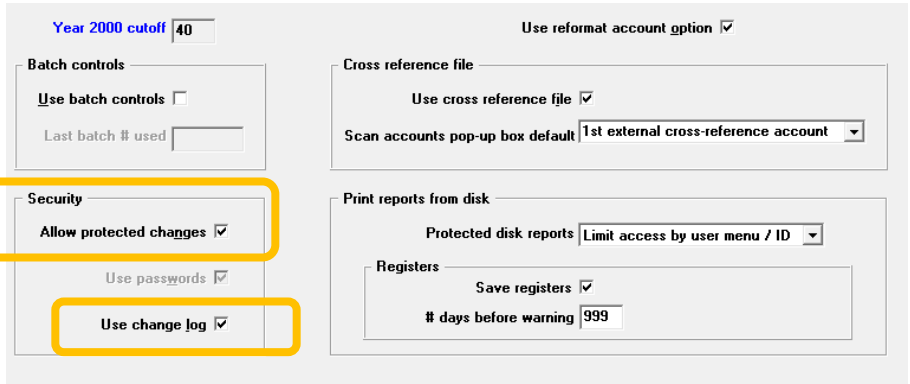
Another area where there is field level security, relates to the ability to change the content of “protected” fields. A protected field is one where the system “expects” to be in full control of the value in that field. Examples include invoice and check numbers where the incrementing of these control numbers is normally under control of the accounting system. However, in certain cases there may be a situation where a user must step in and “force” a change to the pre-set

value. An example might be when a new box of checks is opened and the next check number in the new box does not correspond to the last check number plus one in the old box. Resetting an invoice number may be necessary in the case of certain crashes or other printing or technical problems where an invoice number was used but the system failed to increment the number.

The issue here is, who is allowed to override the value that the system populates in the field and how do you do it? Under normal conditions if you click into this control field, the system will respond with a “Change not allowed” message:



This message came from trying to change the next voucher number in the AP Control file. If the override option has been set to allow overrides, then hitting F2 would allow access to the field – and as a result would change the message in red to “(Allowing protected change)”. In order to preserve some protection from misuse, the information about using the F2 to override is not shown – it must be remembered. This function and protocol are system wide i.e., apply to every protected field that potentially can be changed (some can’t) and the control that allows this is in the Company Control file – Tab 1 General (bottom left corner of screen):

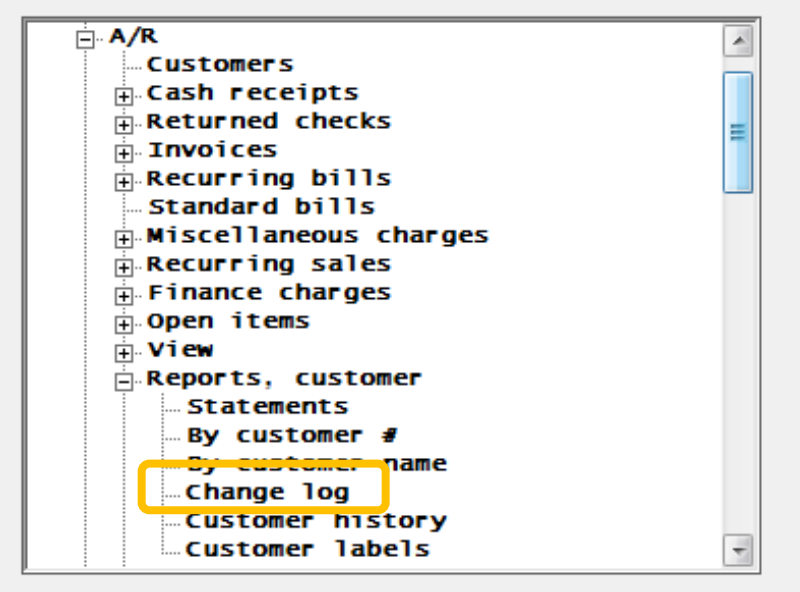


If this control is not set on, then the data field will be unchangeable. Having this data field absolutely unchangeable is probably not the best option because situations do arise where manually changing the value is necessary. However, the most secure kind of compromise is to have this field normally ‘unset’ and then if/when a situation occurs that requires a change, a person with admin privileges can alter this field to set it to on, make the change to the problem data field, then change this field back. This reasonably assumes that the frequency of needing these changes is infrequent. Note here we assume that the Company file maintenance screen shown is only available to admin users through the menu selection options discussed in the prior installment, thus someone with admin privileges only is able to make the change.

Logged Data

Finally, in this field-change security functionality, Passport supports a change log function for all of the of Passport master files – Customers, Vendors, Inventory Items, etc. This function is

turned on in the Company file record – see above. The Change Log will record the “new” image of a newly added record, will record both before and after images of a changed record and will record the deletion of a deleted record. Date and time stamps accompany these images. The report/list program that supports these functions in each application then allows you to review these logged changes and scan them for problematical/suspicious activity. Here is the Change Log print function in AR:



We hope this discussion has provided options and tools for controlling access to the functions of the Passport system, as well as information for logging and protecting important data fields, allowing for a more secure accounting system holding your critical data safely.