



User Guide

PrintStream Security
V21.1.0200

Copyright © 2021 by Electronics for Imaging, Inc. All Rights Reserved.

EFI PrintStream | V21.1.0200 *PrintStream Security User Guide*

This publication is protected by copyright, and all rights are reserved. No part of it may be reproduced or transmitted in any form or by any means for any purpose without express prior written consent from Electronics for Imaging, Inc. Information in this document is subject to change without notice and does not represent a commitment on the part of Electronics for Imaging, Inc.

Patents

This product may be covered by one or more of the following U.S. Patents: 4,716,978, 4,828,056, 4,917,488, 4,941,038, 5,109,241, 5,170,182, 5,212,546, 5,260,878, 5,276,490, 5,278,599, 5,335,040, 5,343,311, 5,398,107, 5,424,754, 5,442,429, 5,459,560, 5,467,446, 5,506,946, 5,517,334, 5,537,516, 5,543,940, 5,553,200, 5,563,689, 5,565,960, 5,583,623, 5,596,416, 5,615,314, 5,619,624, 5,625,712, 5,640,228, 5,666,436, 5,745,657, 5,760,913, 5,799,232, 5,818,645, 5,835,788, 5,859,711, 5,867,179, 5,940,186, 5,959,867, 5,970,174, 5,982,937, 5,995,724, 6,002,795, 6,025,922, 6,035,103, 6,041,200, 6,065,041, 6,112,665, 6,116,707, 6,122,407, 6,134,018, 6,141,120, 6,166,821, 6,173,286, 6,185,335, 6,201,614, 6,215,562, 6,219,155, 6,219,659, 6,222,641, 6,224,048, 6,225,974, 6,226,419, 6,238,105, 6,239,895, 6,256,108, 6,269,190, 6,271,937, 6,278,901, 6,279,009, 6,289,122, 6,292,270, 6,299,063, 6,310,697, 6,321,133, 6,327,047, 6,327,050, 6,327,052, 6,330,071, 6,330,363, 6,331,899, 6,340,975, 6,341,017, 6,341,018, 6,341,307, 6,347,256, 6,348,978, 6,356,359, 6,366,918, 6,369,895, 6,381,036, 6,400,443, 6,429,949, 6,449,393, 6,476,927, 6,490,696, 6,501,565, 6,519,053, 6,539,323, 6,543,871, 6,546,364, 6,549,294, 6,549,300, 6,550,991, 6,552,815, 6,559,958, 6,572,293, 6,590,676, 6,606,165, 6,633,396, 6,636,326, 6,643,317, 6,647,149, 6,657,741, 6,662,199, 6,678,068, 6,707,563, 6,741,262, 6,748,471, 6,753,845, 6,757,436, 6,757,440, 6,778,700, 6,781,596, 6,816,276, 6,825,943, 6,832,865, 6,836,342, RE33,973, RE36,947, D341,131, D406,117, D416,550, D417,864, D419,185, D426,206, D439,851, D444,793.

Trademarks

The APPS logo, AutoCal, Auto-Count, Balance, Best, the Best logo, BESTColor, BioVu, BioWare, ColorPASS, Colorproof, ColorWise, Command WorkStation, CopyNet, Cretachrom, Cretaprint, the Cretaprint logo, Cretaprinter, Cretaroller, DockNet, Digital StoreFront, DocBuilder, DocBuilder Pro, DocStream, DSFdesign Studio, Dynamic Wedge, EDOX, EFI, the EFI logo, Electronics For Imaging, Entrac, EPCount, EPPhoto, EPRegister, EPStatus, Estimate, ExpressPay, Fabrivu, Fast-4, Fiery, the Fiery logo, Fiery Driven, the Fiery Driven logo, Fiery JobFlow, Fiery JobMaster, Fiery Link, Fiery Prints, the Fiery Prints logo, Fiery Spark, FreeForm, Hagen, Inktenity, Inkware, Jetrion, the Jetrion logo, LapNet, Logic, MiniNet, Monarch, MicroPress, OneFlow, Pace, PhotoXposure, PressVu, Printcafe, PrinterSite, PrintFlow, PrintMe, the PrintMe logo, PrintSmith, PrintSmith Site, Printstream, Print to Win, Prograph, PSI, PSI Flexo, Radius, Rastek, the Rastek logo, Remoteproof, RIPChips, RIP-While-Print, Screenproof, SendMe, Sincolor, Splash, Spot-On, TrackNet, UltraPress, UltraTex, UltraVu, UV Series 50, VisualCal, VUTEK, the VUTEK logo, and WebTools are trademarks of Electronics For Imaging, Inc. and/or its wholly owned subsidiaries in the U.S. and/or certain other countries.

All other terms and product names may be trademarks or registered trademarks of their respective owners and are hereby acknowledged.

Table of Contents

- Introduction 4**
 - Overview 4
 - Contact Information 4
- Menus and Users..... 5**
 - Program Groups and Menus 5
 - Users, Security and Roles 9
- Creating Roles and Sub Roles 10**
 - Defining Roles..... 10
 - Defining Sub Roles..... 11
 - Additional Security Levels..... 12
 - Mail Estimating 12
 - Master Files – Inventory..... 12
 - Menu Bar Settings 13
 - Optional Menu Bar Password Setting 13
 - No password options are available - No password changes are allowed 13
 - Lock user account after three login attempts 14
- Security Profiles Reporter 14**
 - User Roles 15
 - Roles Subroles Security Events 16
 - Roles Program Groups and Programs 17
 - Security Events and their Users 18



Introduction

Overview

This guide outlines security rules for PrintStream.

Contact Information

EFI Support

US Phone:	855.334.4457 (first select option 3, then press option 8, then press option 1)
US Fax:	415.233.4157

US E-mail: printstream.support@efi.com

Regular Service Desk hours are 8:00 AM to 7:00 PM Central Time, Monday – Friday. Outside of these hours, you may leave a voice mail message and an on-call support representative will be paged. Response time is based on the severity of the issue.

Note For problems involving infrastructure (i.e., computers, networks, operating systems, backup software, printers, third-party software, etc.), contact the appropriate vendor. EFI cannot support these types of issues.

EFI Professional Services

US Phone:	651.365.5321
US Fax:	651.365.5334

E-Mail: ProfessionalServicesOperations@efi.com

EFI Professional Services can help you perform EFI software installations, upgrades, and updates. This group can also help you implement, customize, and optimize your EFI software plus offer a range of training options.



Menus and Users

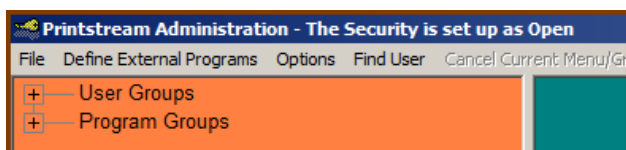
Use this module to add, edit, or delete Users, User Groups, and Programs Groups, and to define and assign Security Roles.

Note The top of the window displays either the **Open** or the **Restricted** security default when this module is open. This setting is created when the database is created and done by EFI PrintStream personnel.

Open: When defining the Security Events to which users in a Sub Role may access, means that what you see are **ONLY** the items to which users in that Sub role do **NOT** have access. In other words, Open dictates that other access is allowed. If you give a user access to an executable program – that user will have full access unless a security event is set to restrict them from a field or function.

Restricted-Closed: When defining the Security Events to which users in a Sub Role may have access, means that what you see are **ONLY** the items to which users in that Sub Role **WILL** have access. In other words, Restrictive dictates that other access is denied.

As is common in most security systems, if 2 Sub Roles conflict and a Role has BOTH Sub Roles, access will be permitted to that security event. In this case: Open and Restrictive do not pertain.



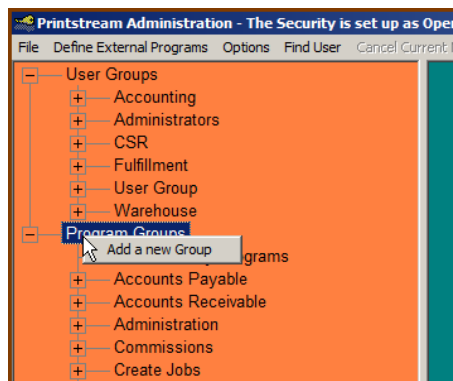
Program Groups and Menus

Program Groups are the categories or groups you see on the PrintStream menu bar. Underneath each Program Group are the executable programs assigned to the group the users can access if they have security access.

To create a new program group

1. Right-click Program Groups and select Add a New Group.
2. Enter a name.

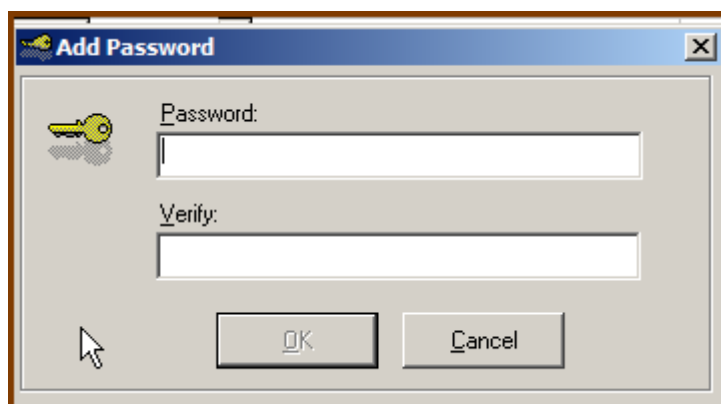
This name appears in the list under Program Groups, and as a gray bar on any Menu Bar that includes this program group.



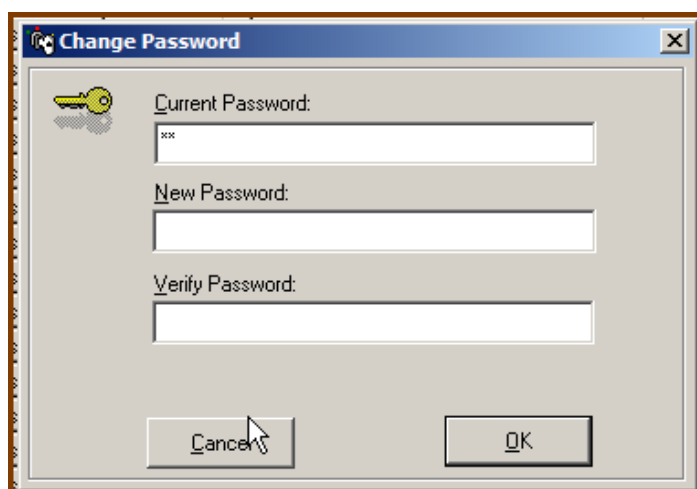
6. When you update programs, you will see a list of executable programs available to select from. The programs listed at the top with the red check are the programs already activated for this program group. The remainder of the programs available are listed alphabetically. You can change the name of the program listed under **Display Name**, save the changes, and the new name is displayed on the PrintStream menu bar. The executable name cannot be edited.

Each program has a security level of 0-5 assigned to it. When setting up users, a security level of 0-5 is assigned to each individual. If the security level of a program is the same as or greater than the security level of the employee, the individual is able to see/access those programs. For example, a user with a number of zero can see all programs. A user with number 3 only has access to programs with a number 3, 4 or 5. A user with a 5 can only see programs assigned a 5.

7. To change the order the programs appear when a user logs in, use your mouse to drag and drop the programs on the left side of the screen under Program Group.
8. For additional security, you can also assign a password to a program. Select the **Add Password** button next to the program and assign a password. There are no restrictions when setting up this password. Once a password has been assigned to a program, the button changes from **Add Password** to **Change Password**.



9. If you wish to remove a password setup for a program, select the **Change Password** button. Leave the **New Password** and **Verify Password** fields blank and click **OK**.



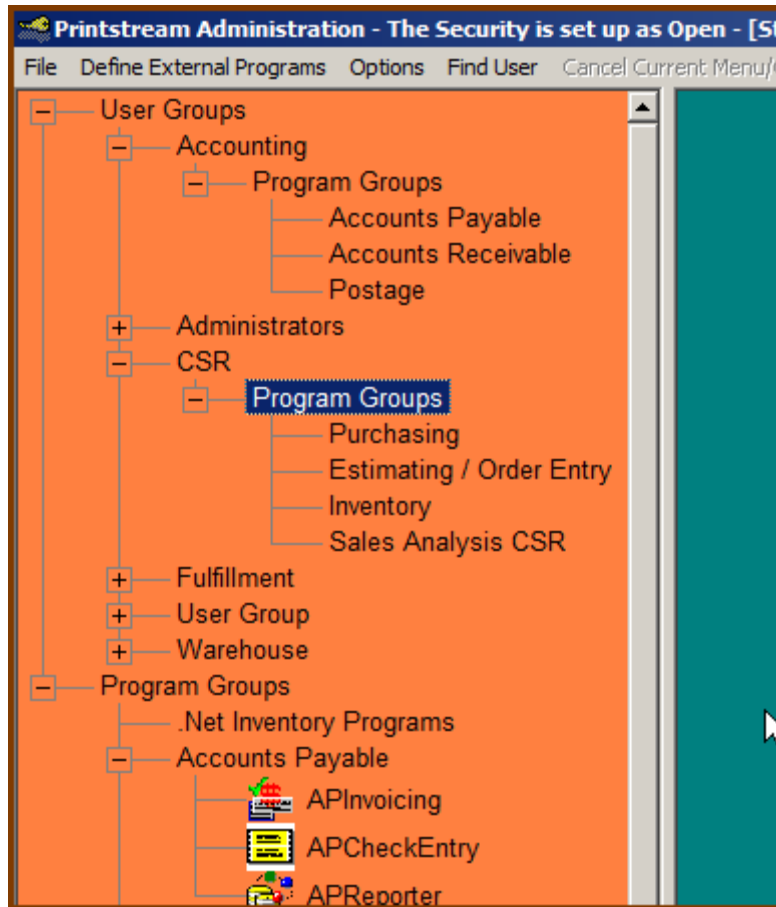
User Groups define the collection of Program Groups a user sees when they log into PrintStream.

To create or edit this list

1. Right-click **User Groups** and select **Add a New Menu**.
2. Enter the desired name, which displays in the list under User Groups.

Under each **User Group** name is the heading **Program Groups**, and a listing of the Program Groups that fall under that user group.

3. Drag-and-drop from the list of Program Groups to this heading to add any Program Group to any **User Group** as well as move their listing order around. Right-click to rename, select Update, or delete.



Users, Security and Roles

To add users

1. Select File > Add User.
2. Enter the desired login name and password, plus the user's full name, optional email address, security level and/or permission to change the database path
3. Click the box next to the company for access and select the role
4. Click Save.
5. View existing users from the Find User menu option.
6. Double-click any name to bring up the same entry window in order to edit or delete a particular user.

	Company Code	Plant Code	Role
1	01	0100	

To set Password Restrictions, see Menu Bar Settings instructions below.

Each user must be assigned to one or more facilities and given one Role for each assigned facility. A user's Role links them to a User Group because each Role is assigned a User Group. The user has access to all programs in the User Group connected to their assigned Role that have the same, or a lower, security level than the user.

Each Role is linked to one or more Sub Roles. The user can be restricted from functions within any program they have access to based upon the Sub Roles linked to their assigned Role.

Creating Roles and Sub Roles

Define Roles and Sub Roles using the Security menu option from the Menu and Users program.

Defining Roles

To access Roles, select **Security > Roles**. The Role window lists all existing Roles. Highlight any Role to view the User Group to which it is assigned (displayed under the tab Role), and the associated users (displayed under the tab User).

To create a new Role

1. Select **Add Role**.
2. Enter a **Role Name** and select a **User Group**.
3. Select the desired **Sub Roles** check box and click **Save**.

Right-click any Role to select Delete.

Roles

Action

Role List

- Accounting
- Acctg A/R & A/P
- Administrators
- CSR**
- CUSTWEBVIEW
- CUSTWEBVIEW2
- Estimating
- FFAdmin
- FFW_IR
- Human Resources
- Inventory
- Kris
- MF-Customer - read only
- MF-Inv. Read only
- No MFI
- Postage
- Sales
- Scheduler
- Shop Floor
- TestCelia
- Web

Role (tab) | Users (tab)

Role Name: CSR

User Group (Menu): Sales & Customer Service

Sub Roles:

- ☒ CSR
- ☐ CUSTWEB
- ☐ CUSTWEB2
- ☐ CUSTWEBALL
- ☐ edit costs on invoiced jobs
- ☐ Everything
- ☐ FFW_IR
- ☐ Fulfillment
- ☐ Inv Kris
- ☐ Invenftestcelia
- ☐ Kris
- ☐ MF-Customer - Limited Access
- ☐ MF-Inv Read only
- ☐ no MFI
- ☐ Read only scheduling
- ☐ Support
- ☐ Test
- ☐ test restrictions

Close Add Role Save

Defining Sub Roles

To access sub role information, select **Security > Sub Roles**.

Sub Roles allow functions within programs to be made invisible to users.

To view current Sub Role status

1. Highlight any Sub Role listed under the **Sub Roles** tab.
All existing security definitions for this Sub Role display.
2. Two control types are currently available:
 - a. **Read:** means a user can see the function.
 - b. **Write:** means a user can make data changes in the function.
3. Select a check box to determine the function is active or click **Select All** or **Deselect All**.

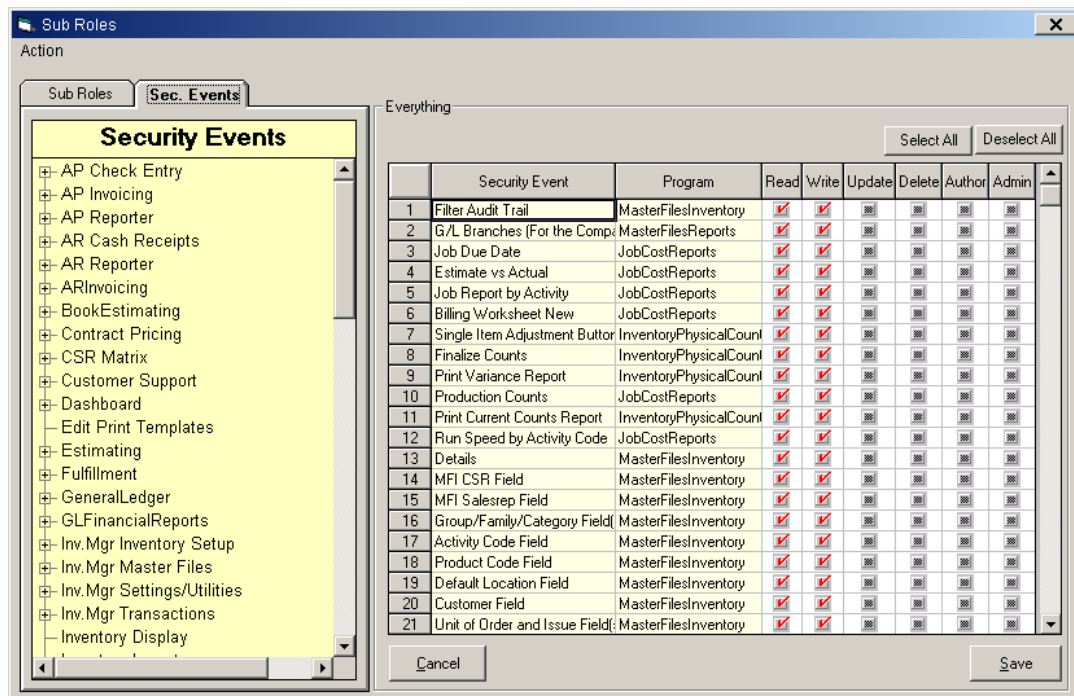
To create new Sub Roles

1. Select **Action** and then **Add Sub Role**.
2. Enter the desired name.

To define or edit a Sub Role, highlight the Sub role in the Sub Roles List under the Sub Role tab. The name of the highlighted Sub Role displays in the top center of the window.

3. Select the **Sec. Events** tab.

All of the security events currently defined for this Sub Role display and can be edited.



4. Right-click a single line to delete that line or all lines.
5. To add additional security functions for the selected Sub Role, go to the list under the heading Security Events (left side of window). The top level of this list consists of the program. Below this level are functions within each program. Highlight either an entire program, or a subset of functions within that program or a single function within the program. Right-click and click **Add me to the Sub Role**.

Note The original choice of Open or Restricted access impacts the necessary action when defining Sub Roles. A choice of Open means that when a new Sub Role is created, you must select those functions within a program which a user will be denied access. When program functions are added to the Sub Role list, they default to off, however they can be checked to on. All program functions not selected to define security default to on.

A choice of **Restricted** means that when a new Sub Role is created, you must select those functions within a program which a user is allowed access. Any program functions added to the Sub Role list default to on, however they can be unchecked to off. All program functions not selected to define security default to off.

As is common in most security systems, if 2 Sub Roles conflict and a Role has BOTH Sub Roles – access is permitted to that security event. In this case, **Open** and **Restrictive** do not pertain.

Additional Security Levels

A 0 represents the highest level of security (most access) and a 5 represents the lowest level of security (least access).

Mail Estimating

If a user security level =

- 5 – Users do NOT have access to the **Final Pricing** screen, **Quote Letter**, and **Mail Quote Breakdown**.
- 4 or 3 – Users do NOT have access to **override pricing** in the **Final Pricing** screen.
- 2, 1 or 0 – Users have FULL access to **override pricing** in the **Final Pricing** screen.

Master Files – Inventory

If a user security level =

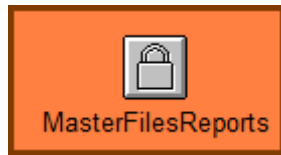
- 5 – Users have VIEW ONLY access, cannot edit inventory codes or descriptions, and cannot create new inventory items.

Note If you do NOT want a user to view a module within a program group (e.g., Master File – Mail Process or Master File – Print), make their user security number a higher number than the program security number. Program security numbers are maintained when you update Program Groups. When changed, they apply to all Program Groups to which the program has been associated. Changes take effect when you close out of PrintStream and log back into the system.

Menu Bar Settings

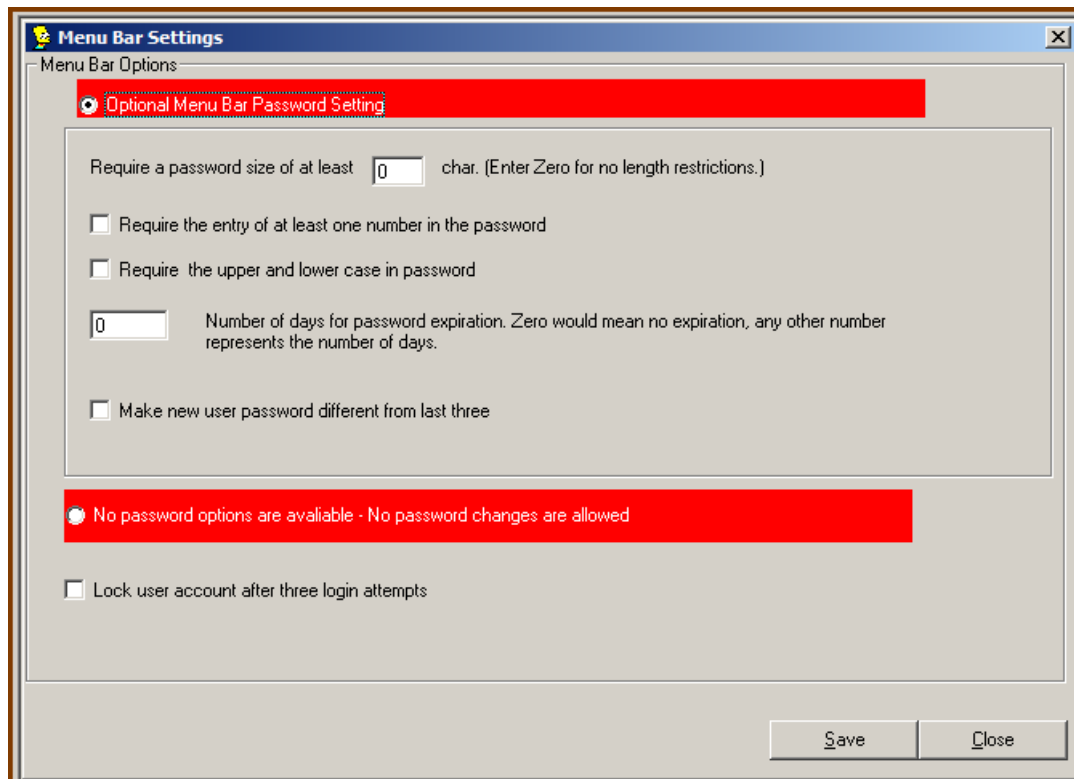
This program allows you to set password restrictions.

1. Go to **Master Files Reports > System Maintenance> Menu Bar Settings**.



2. Enter the password.

A password is required for this program. Please contact your EFI PrintStream Support contact if you do not know this password.



Optional Menu Bar Password Setting

By selecting the **Optional Menu Bar Password Settings** option, you are indicating users have the option to modify their own password through the menu bar.

You can set a minimum password length. If you leave it as zero, it has no length restrictions.

Select if you want to require the entry of at least one number and/or to require an upper and a lower case in the password.

Set the number of days for password expiration and make new user password different from last three.

No password options are available - No password changes are allowed

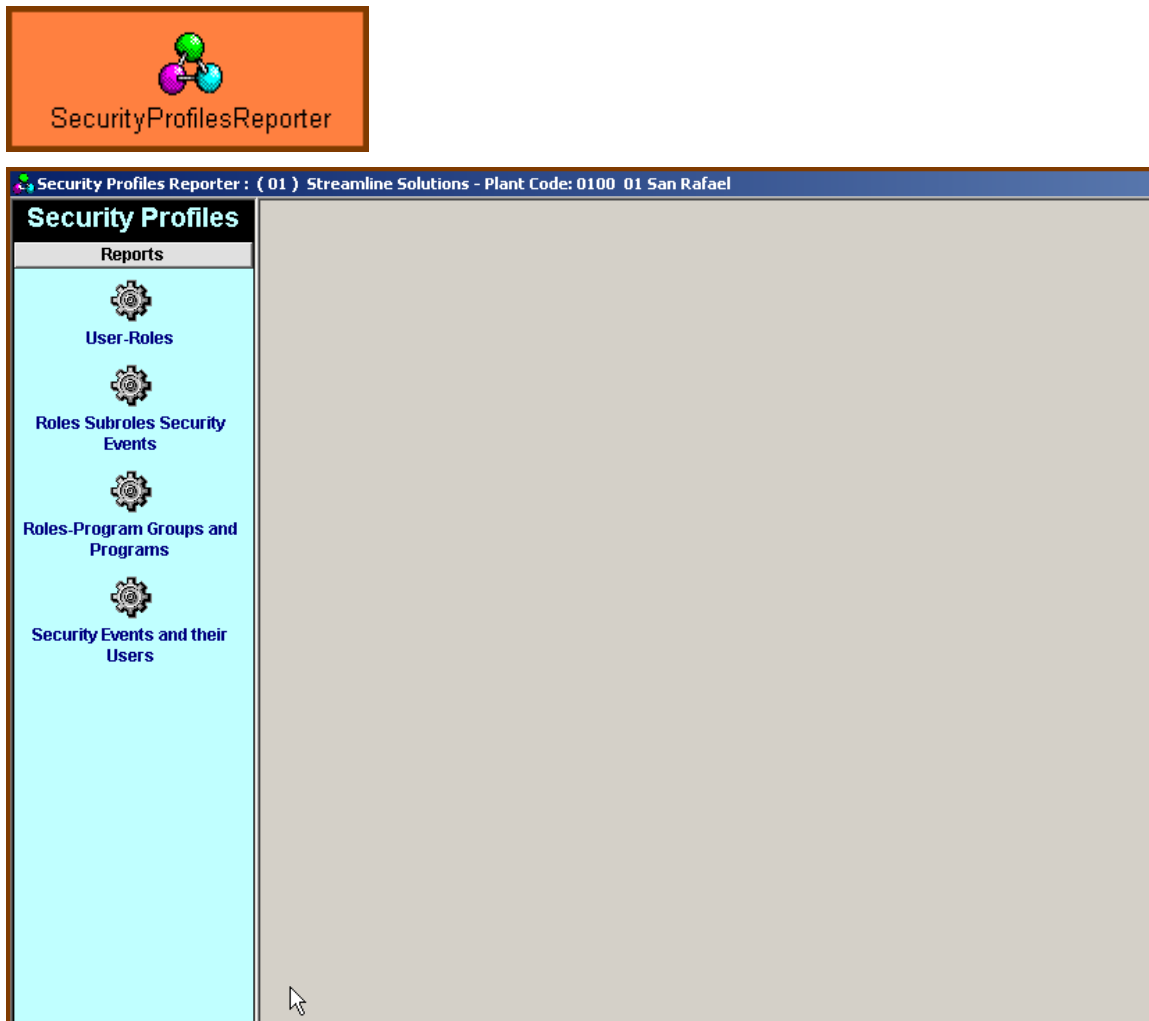
This means that passwords can only be changed from the Menus and Users program.

Lock user account after three login attempts

This setting can be used if **Optional Menu Bar password** is selected or not. If a user fails to enter a valid password while logging in after 3 attempts, they are locked out. The only way to fix that password would be to do so from menus and users.

Security Profiles Reporter

The security profiles reporter gives you the option to print various reports based on user setup and access.



User Roles

User Roles allows you to run a report of one user (or all) or one role (or all) and shows the user, role, and the Program Groups that user is allowed into. It also shows which companies and plants the user has access to if the **Print for All Companies/Plants** is selected.

User-Roles

Select User (Leave blank for all)

Select Role (Leave blank for all)

☐ Print for all Company/Plants

Close Print

Streamline Solutions

User-Roles Report

Page 1 of 11

For User: <All> Printed: 7/13/2010 1:48:49PM
For Role: <All> By: LS

UserID	User Name	Active	Company	Plant	Role	Program Groups
1234	Flowers R Us	Yes	01	0100	CUSTVIEW	Fulfillment
acct	Accounting test	Yes	01	0100	Accounting	Accounts Payable Accounts Receivable Postage
Administrator	Administrator	Yes	01	0100	Administrators	Master Files Administration Estimating / Order Entry Purchasing Shop Floor Job Costing Inventory Postage Sales Analysis Accounts Receivable Accounts Payable General Ledger and Financials Printstream Scheduler Fulfillment Web Style Create Jobs Commissions .Net Inventory Programs
ASPNET	WEBIMPORTS	Yes	01	0100	Administrators	Master Files Administration Estimating / Order Entry Purchasing Shop Floor Job Costing Inventory Postage Sales Analysis Accounts Receivable Accounts Payable General Ledger and Financials Printstream Scheduler Fulfillment Web Style Create Jobs Commissions .Net Inventory Programs
bill	Bill M	Yes	01	0100	Administrators	Master Files

Roles Subroles Security Events

The **Roles Subroles Security Events** report allows you to see Roles and the subroles under them as well as the read/write access of each subrole security event. This report can be run for all roles, one role, or one user. Security Event Detail is optional.

Roles Subroles Security Events

Selection

☒ Print for all Roles

☐ Filter By Role:

☐ Filter By User:

☒ Print Security Event detail

Streamline Solutions

Roles Subroles Security Events Report Page 1 of 80

For User: <All> Printed: 7/13/2010 1:51:52PM

For Role: <All> By: LS

Role	Sub_Roles	Security Events	Read	Write	Update	Delete	Author	Admin
Accounting	Everything	1099 FIELD(S)	Y	Y				
		A/P BATCH DISPLAY	Y	Y				
		A/P BATCH TRANSACTION	Y	Y				
		A/P DISSECTION CODE REPORT	Y	Y				
		A/P DISPLAY	Y	Y				
		A/P FUTURE CASH REQUIREMENTS	Y	Y				
		A/P INVOICES BY DATE	Y	Y				
		A/P INVOICES PAID BY DATE AND DISS. CODE	Y	Y				
		A/P MONTH END CALCULATION	Y	Y				
		A/P PAYMENT SUMMARY	Y	Y				
		A/P PURCHASE ORDERS	Y	Y				
		A/P RECONCILIATION	Y	Y				
		A/P SUMMARY AND DETAILED AGING	Y	Y				
		A/P TRANSACTIONS BY DATE	Y	Y				
		A/R AGING REPORT	Y	Y				
		A/R BANK DEPOSIT SLIP	Y	Y				
		A/R BATCH TRANSACTION	Y	Y				
		A/R DETAILED SUSPENSE	Y	Y				
		A/R MONTH END CALCULATION	Y	Y				
		A/R RECONCILIATION	Y	Y				
		A/R TRANSACTIONS BY DATE	Y	Y				
		ACCOUNTING PERIODS	Y	Y				
		ACCOUNTS START PERIODS	Y	Y				
		ACCRUALS BATCH ENTRY	Y	Y				
		ACTION CHART	Y	Y				
		ACTIVITIES(FOR THE SYSTEM)	Y	Y				
		ACTIVITY CODE FIELD	Y	Y				
		ACTIVITY CODES	Y	Y				
		ACTIVITY FILE TO GL REPORT	Y	Y				
		ADD / EDIT / DELETE SALESREP	Y	Y				
		ADD EMPLOYEE	Y	Y				

Roles Program Groups and Programs

The **Roles-Program Groups and Programs** report shows you the role, which program groups are under that role, which executable programs under that program group, the security level of the program, and if it is password protected. This report can be run for all roles, one role, or for one user.

Streamline Solutions

Page 1 of 15

For User: <All> Printed: 7/13/2010 1:54:01PM
For Role: <All> By: LS

Role	Program Group	Programs	Program Priority	Password Protected	Executable Name
Accounting	Accounts Payable	AP Invoicing	5		APINVOICING.EXE
		AP Check Entry	5		APCHECKENTRY.EXE
		AP Reporter	5		APREPORTER.EXE
	Accounts Receivable	AR Invoicing Entry	5		ARINVOICINGENTRY.EXE
		AR Cash Receipts	5		ARCASHRECEPTS.EXE
		AR Reporter	5		ARREPORTER.EXE
		AR Display	5		ARDISPLAY.EXE
		AR Cross Reference	5		ARCROSSREFERENCE.EXE
		Commissions Report	5		COMMISSIONSREPORT.EXE
		AR Customer Collection	5		ARCUSTOMERCOLLECTION.EXE
		AR Database Builder	5		ARDATABASEBUILDER.EXE
		AR Price List Invoicing	5		ARPRICELISTINVOICING.EXE
		Contract Pricing	5		CONTRACTPRICING.EXE
		Industry Performance Profile	5		INDUSTRYPERFORMANCEPROFILE.EXE
		ICC_Prebill	5		ICC_PREBILL.EXE
		AR Invoicing Import	5		ARINVOICINGIMPORT.EXE
		Commissions Auto	5		COMMISSIONSAUTO.EXE
	Postage	Postage Entry	5		POSTAGEENTRY.EXE
		Postage Receipt Allocations	5		POSTAGERECEIPTALLOCATIONS.EXE
		Master Files Postage Inventory	5		MASTERFILESPOSTAGEINVENTORY.EXE
		Postage Adv Invoice	5		POSTAGEADVANCEDLLTR.EXE
		Postage Audit Adjustment	5		POSTAGEAUDITADJUSTMENT.EXE
		Postage Inventory Adjustment	5		POSTAGEINVENTORYADJUSTMENT.EXE
		MDD Support	5		MDDSUPPORT.EXE
		Postage Purge To purge 3602 etc.	5		POSTAGEPURGE.EXE
		Postage Recap	5		POSTAGERECAP.EXE
		Postage Statements Reporter	5		POSTAGESTATEMENTSREPORTER.EXE
		Postage Reporter	5		POSTAGEREPORTER.EXE
		Postage Statements	5		POSTAGESTATEMENTS.EXE
		Postage Grid Entry	5		POSTAGEGRIDENTRY.EXE
		EPI	5		EPI.EXE
		Mail Dat User Interface	5		MAILDATUSERINTERFACE.EXE
Administrators	Master Files	Master Files Reports	5		MASTERFILESREPORTS.EXE
		Master Files Mail Process	1		MASTERFILESMAILPROCESS.EXE
		Master Files Customer	5		MASTERFILESCUSTOMER.EXE
		Master Files Vendor	5		MASTERFILESVENDOR.EXE
		Master Files Employee	5		MASTERFILESEMPLOYEE.EXE
		Master Files Inventory	5		MASTERFILESINVENTORY.EXE
		Master Files Print	2		MASTERFILESPRINT.EXE
		Master Files Stk Header	5		MASTERFILESSTKHEADER.EXE
		Master Files Postage Inventory	5		MASTERFILESPOSTAGEINVENTORY.EXE
		Master Files Signature	5		MASTERFILESSIGNATURE.EXE
		Master File Product	5		MASTERFILEPRODUCT.EXE
		Master Files Book	5		MASTERFILESBOOK.EXE
		Master Files Book QL	5		MASTERFILESBOOKQL.EXE
		Master Files Colors	5		MASTERFILESCOLORS.EXE

Security Events and their Users

The **Security Events and their Users** report allows you to see one security event (or all) and which users have access to this event.

Streamline Solutions

Security Events and their Users

Page 1 of 912

For Sec. Event: <All> Printed: 7/13/2010 2:58:48PM
By: LS

Security Event	Sub-Role	UserID	Cmpny	Plant	Read	Write	Update	Delete	Author	Admin
1099 FIELD(S)	Everything	acct	01	0100	Y	Y				
	Everything	acct	02	0200	Y	Y				
	Everything	Administrator	01	0100	Y	Y				
	Everything	ASPNET	01	0100	Y	Y				
	Everything	ASPNET	02	0200	Y	Y				
	Everything	bill	01	0100	Y	Y				
	Everything	bill	02	0200	Y	Y				
	Everything	Bob	01	0100	Y	Y				
	Everything	brian	01	0100	Y	Y				
	Everything	brian	02	0200	Y	Y				
	Everything	Cbannon	01	0100	Y	Y				
	Everything	cecylia	01	0100	Y	Y				
	Everything	Chris	02	0200	Y	Y				
	Everything	Dennis	01	0100	Y	Y				
	Everything	dk	01	0100	Y	Y				
	Everything	dk	02	0200	Y	Y				
	Everything	dmm	01	0100	Y	Y				
	Everything	ginao	01	0100	Y	Y				
	Everything	ginao	02	0200	Y	Y				
	Everything	jason	01	0100	Y	Y				
	Everything	jason	02	0200	Y	Y				
	Everything	jocondon	01	0100	Y	Y				
	Everything	Joe	01	0100	Y	Y				
	Everything	john	01	0100	Y	Y				
	Everything	john	02	0200	Y	Y				
	Everything	kathy	01	0100	Y	Y				
	Everything	kathy	02	0200	Y	Y				
	Everything	kb	01	0100	Y	Y				
	Everything	kris	01	0100	Y	Y				
	Everything	kris	02	0200	Y	Y				
	Everything	leah	01	0100	Y	Y				
	Everything	leah	02	0200	Y	Y				
	Everything	lp	01	0100	Y	Y				
	Everything	lp	02	0200	Y	Y				
	Everything	LS	01	0100	Y	Y				
	Everything	mark	01	0100	Y	Y				
	Everything	md	01	0100	Y	Y				
	Everything	norma	01	0100	Y	Y				
	Everything	norma	02	0200	Y	Y				
	Everything	PS	02	0200	Y	Y				
	Everything	Rob	01	0100	Y	Y				
	Everything	sheelah	01	0100	Y	Y				