SYSPRO and the Sarbanes-Oxley Act

How to use SYSPRO to assist in becoming Sarbanes-Oxley compliant.

June 2011

Enterprise Software Solutions for Manufacturers and Distributors

www.syspro.com 1 800 369 8649 info@us.syspro.com

Table of Contents

Executive overview **3**

Sarbanes-Oxley Act **3**

- Segregation of Duties 4
- Integrity of Operations 4
- Auditability 4

SYSPRO and Sarbanes-Oxley **5**

- Account provisioning with segregation of duties 6
- Integrity of Operations 17
  - Controls for change management 17
  - Controls for software updates 17
  - Understanding key system configurations 18
- Auditability 18
  - Reviewing audit logs 18
  - Identifying abnormal transactions in a timely manner 21
  - Archiving and retrieval of reports and documents 22

Summary **23**

Executive overview

The aim of the Sarbanes-Oxley Act is to protect investors and increase investor confidence in American companies. It was established in the wake of corporate scandals such as Enron and WorldCom. The Act tries to instill in companies the concept of good corporate governance.

The Act affects all American listed companies, their divisions, and wholly owned subsidiaries as well as non-US public multi-national companies doing business in the US.

Enterprise Resource Planning (ERP) software cannot be classed as Sarbanes-Oxley compliant per se, as there is no compliancy certification standard for software. However, it can assist a company in its endeavors to become and remain compliant.

The main areas where ERP software packages can be of use to companies in becoming Sarbanes-Oxley compliant are by assisting with *Segregation of Duties*, ensuring *Integrity of Operations* and *Auditability*. SYSPRO can assist in attainment of compliancy by making the data more accessible, transparent and by highlighting exceptions timeously.

The remainder of this document details the five most common IT control weaknesses, and explains how SYSPRO can be configured to alleviate them.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act (or the “U.S. Public Company Accounting Reform and Investor Protection Act of 2002, to give it its correct name) tries to instill in companies the concept of good corporate governance. This means that companies obey all of the required laws and regulatory demands. Good corporate governance is not intended to prevent companies from making a profit but rather to instill the concept of “Performance with Integrity”. Companies are expected to have suitable controls over its people, processes and applications so that its financial reports can be prepared within the guidelines of GAAP and IFRS requirements.

Segregation of Duties

The following definition of “Segregation of Duties” is from The Information Security Glossary :

“*A method of working whereby tasks are apportioned between different members of staff in order to reduce the scope for error and fraud. For example, users who create data are not permitted to authorize processing; Systems Development staff are not allowed to be involved with live operations.*

This approach will not eliminate collusion between members of staff in different areas, but is a deterrent. In addition, the segregation of duties provides a safeguard to your staff and contractors against the possibility of unintentional damage through accident or incompetence - 'what they are not able to do (on the system) they cannot be blamed for'.”

This is normal good business practice, but the level to which the duties can be segregated is dependent on the number and quality of available staff. In a large company there may be ten or more Accounts Payable staff; in this case it is easy to specify who can post invoices, who can assign payments and who authorizes them. In a company or branch with only one A/P clerk this is not so easy, and other controls must be put in place to mitigate the risks. However, you also need to be able to prove that these controls are in place.

Where other products are designed around SYSPRO, or customization takes place, these developers must not have access to the main application server. This development must happen on a separate system, be tested and then deployed to the application server.

Integrity of Operations

Integrity of Operations is being able to state “who did what”, and be able to prove that it was that operator that performed the task. Each operator must have their own SYSPRO login and password. If operators know each other’s logins and passwords, how are you going to prove which one performed a task? In addition, System Administrators must not have access to the accounts of others, as they will be able to commit fraud, and hide it.

Within SYSPRO you can specify which operator codes belong to which operator groups. Against an operator group you specify which programs can be run, and if the program contains a browse you can specify if only the browse can be run. Against the operator code you can restrict access to specific warehouses, branches and banks. Where a program has many options such as posting invoices / credit notes / debit notes it is possible to restrict which of these activities can be performed by an operator, as well as restrict access to specific fields such as inventory costs.

There are many areas that can also be restricted using passwords. In addition, the eSignature system can be configured to lock down the system even more.

Auditability

“Auditability” is being able to prove what happened, even if it was a long time ago. This means keeping older data either on file, or archiving it in a way that it can be retrieved when required. SYSPRO has built in archive capability including the audit trails in posting programs and amendment journal programs for primary data take-on programs. SYSPRO Electronic Signature system can be configured to log more detailed transactions.

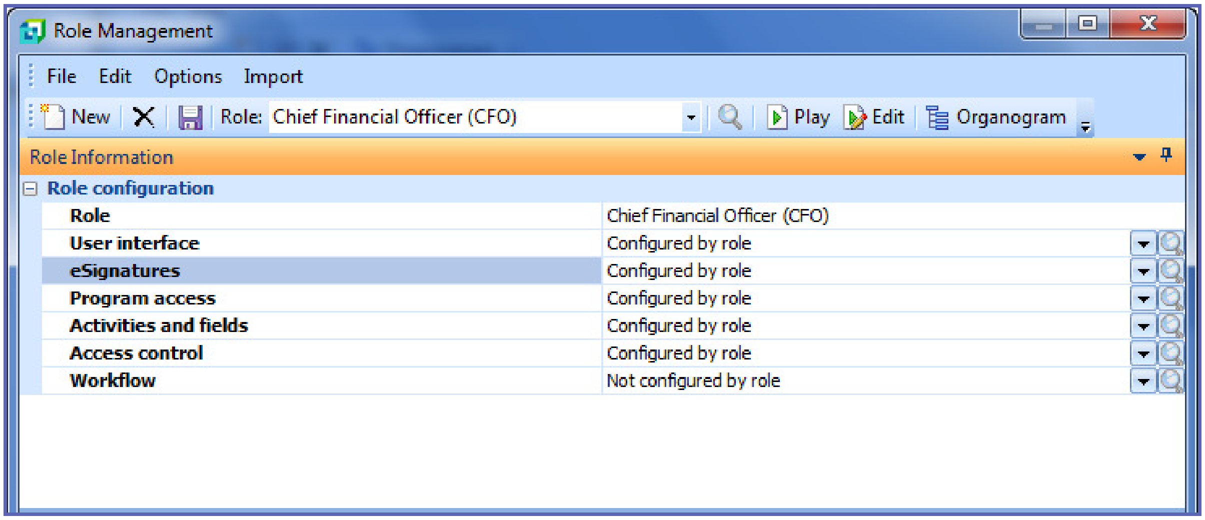
SYSPRO and Sarbanes-Oxley

In April 2005, CIO magazine listed the five most common IT control weaknesses with regard to Sarbanes-Oxley (http://www.cio.com/blog_view.html?CID=4282) and (http://www.cio.com/archive/070105/sox_sidebar_two.html). These are –

1. Improper account provisioning with segregation of duties
2. Insufficient controls for change management
3. A general lack of understanding around key system configurations
4. Audit logs not being reviewed (or that review itself not being logged)
5. Abnormal transactions not identified in a timely manner

Rather than list out all the functions and facilities within SYSPRO that can affect compliancy, this document explains how SYSPRO helps alleviate these five weaknesses.

It would be prudent, at this point, to briefly define the security hierarchy within SYSPRO. The employees of an organization are termed operators in SYSPRO. Operators are always assigned to a group and may optionally be assigned to a role. It is recommended that SYSPRO always be implemented using roles as it provides the optimum security and controls for an organization. Additionally, roles provide a simplified means for a system administrator to pre-configure and control the user interface, electronic signature settings, as well as access to programs, activities, fields, etc. that are presented to SYSPRO operators. By assigning operators to roles, the process of managing security settings is defined once against the role, rather than against each individual operator. This makes managing security more efficient for a large number of operators when new operators need to be added or when operators are re-assigned to a different part of the organization.



Role: Chief Financial Officer (CFO)

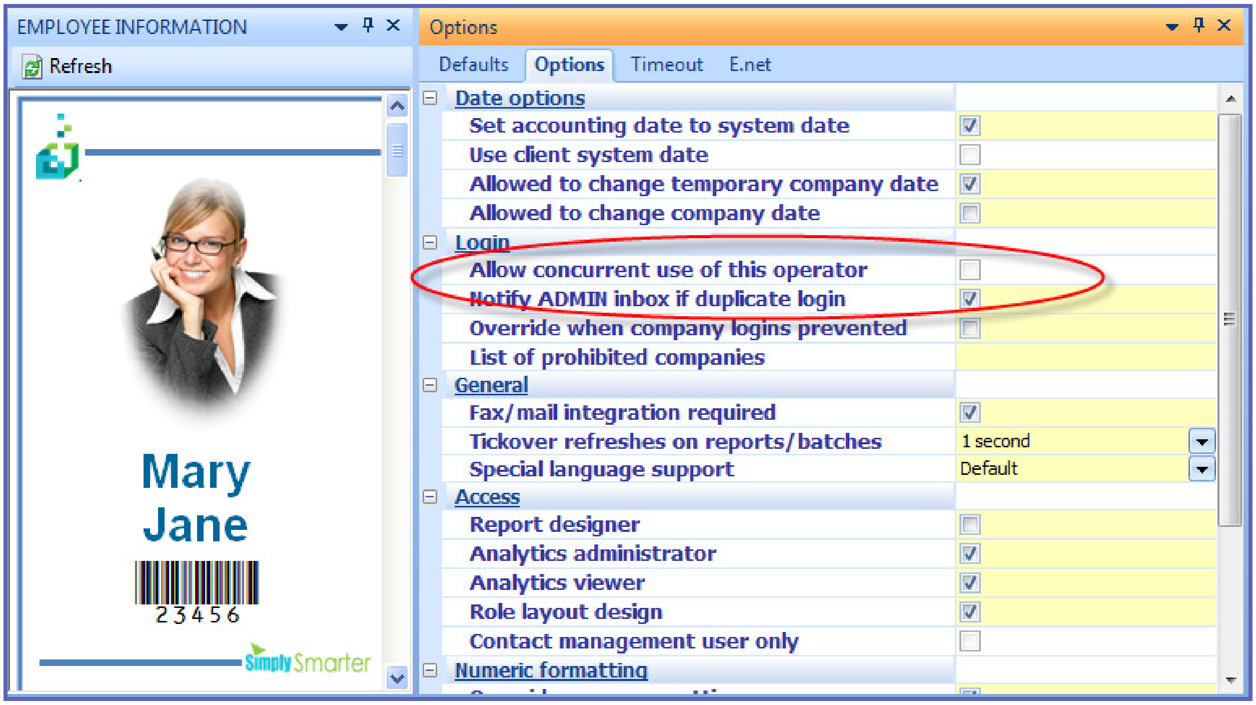
Role configuration

Role	Chief Financial Officer (CFO)
User interface	Configured by role
eSignatures	Configured by role
Program access	Configured by role
Activities and fields	Configured by role
Access control	Configured by role
Workflow	Not configured by role

Account provisioning with segregation of duties

Each operator must have their own operator code (user name) and password. This should not be negotiable. There is no reason for users to share operator codes, and the password should be secret to the operator. The System Administrator should not know the passwords of other operators. If the Administrator knows other operators' passwords, there would be no way to prove that a specific operator performed a task, or to prevent this Administrator from posting a transaction using one operator code and authorizing it using another.

Do not allow concurrent use of an operator (This option is disabled by default when a new operator is created).



Date options
- Set accounting date to system date ☑
- Use client system date □
- Allowed to change temporary company date ☑
- Allowed to change company date □

Login
- Allow concurrent use of this operator □
- Notify ADMIN inbox if duplicate login ☑
- Override when company logins prevented □
- List of prohibited companies

General
- Fax/mail integration required ☑
- Tickover refreshes on reports/batches: 1 second
- Special language support: Default

Access
- Report designer □
- Analytics administrator ☑
- Analytics viewer ☑
- Role layout design ☑
- Contact management user only □

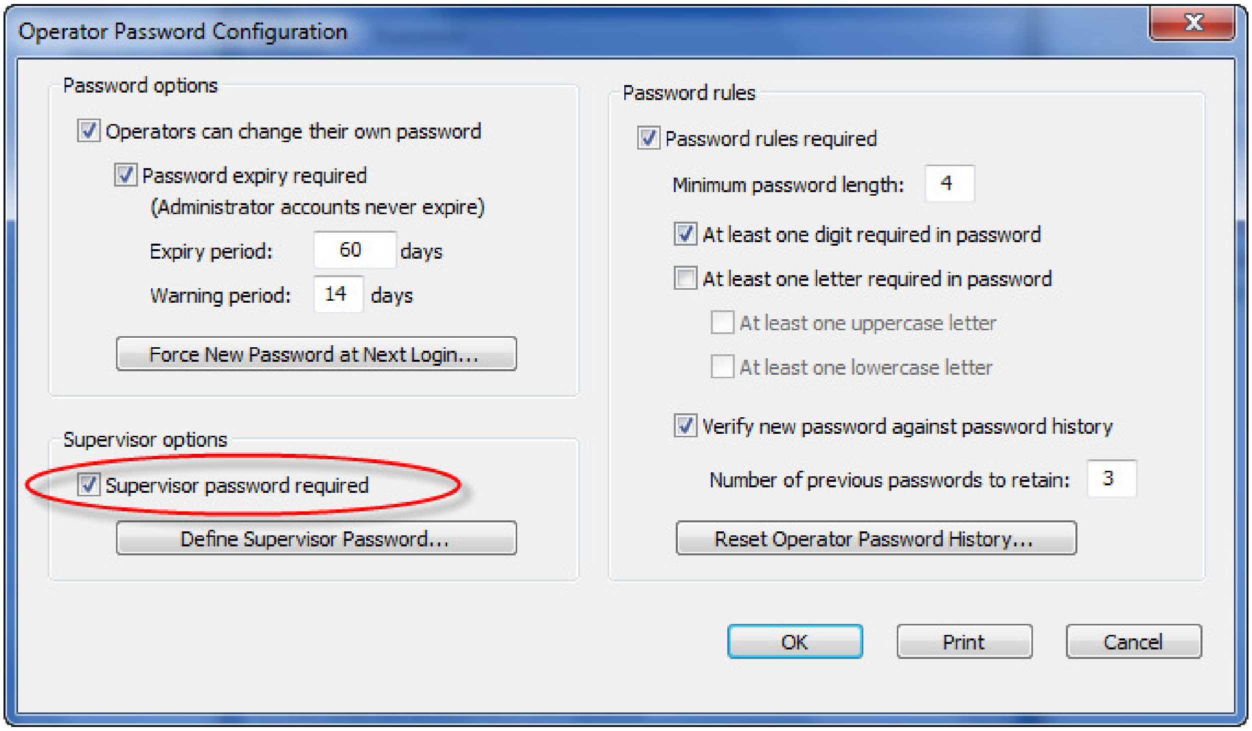
Numeric formatting

Some operators will claim that they need to be able to run multiple instances of SYSPRO to perform multiple tasks concurrently. With SYSPRO operators are allowed to run multiple occurrences of SYSPRO from the same login instance. This means that only one SYSPRO login occurs and you can fire up multiple sessions from the SYSPRO menu. These can be for the same (or different) company IDs. The additional occurrences do not increase the license count as they do not perform an additional login. This facility removes the requirement to allow multiple logins with the same operator code. This feature is available by default; no additional flags, options or security settings are necessary.

An organization can optionally enable the supervisor option: "Supervisor password required". With this option you can configure a password that allows the Administrator to override all operator passwords. If the Administrator attempts to log in as another operator code they can supply this password instead of the operator's password and they will be allowed to perform any task that the original operator can perform. The job logging will reflect that it was performed by the original operator and not the Administrator, however the system audit log will reflect that the supervisor password was used to log in as that operator.

Note: It is therefore crucial that someone other than the "supervisor", who is typically the SYSPRO system administrator, reviews these system audit logs.

Whenever an option is changed on the password setup screen (or any setup screen) it will be reflected on the system amendment journal, including flagging the option to have a supervisor password.


Operator Password Configuration

Password options

☑ Operators can change their own password

☑ Password expiry required
(Administrator accounts never expire)

Expiry period: 60 days

Warning period: 14 days

Force New Password at Next Login...

Supervisor options

☑ Supervisor password required

Define Supervisor Password...

Password rules

☑ Password rules required

Minimum password length: 4

☑ At least one digit required in password

☐ At least one letter required in password

☐ At least one uppercase letter

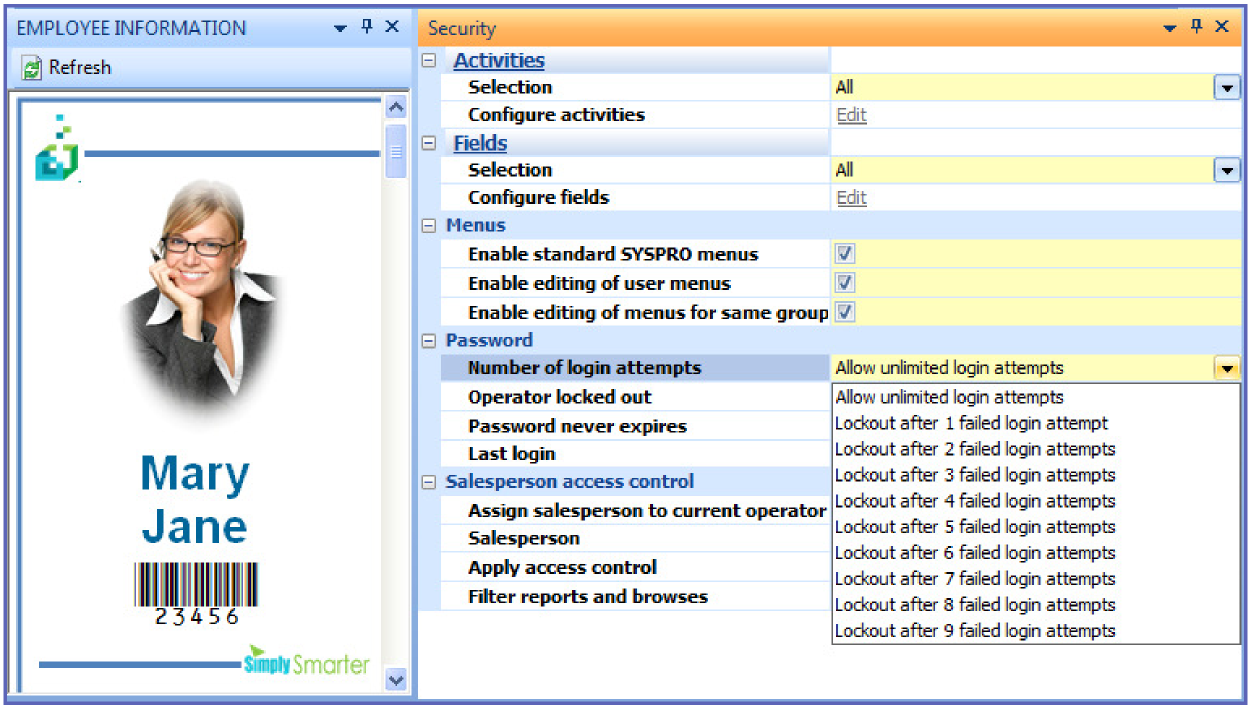
☐ At least one lowercase letter

☑ Verify new password against password history

Number of previous passwords to retain: 3

This screen also allows you to set up your password rules. You can set how often a password needs to be changed, as well as the make-up of this password. Research has shown that if you make the password rules too cumbersome (complex passwords and frequent changes), operators will start writing them down as reminders. This poses a greater security risk than a more lenient password policy.

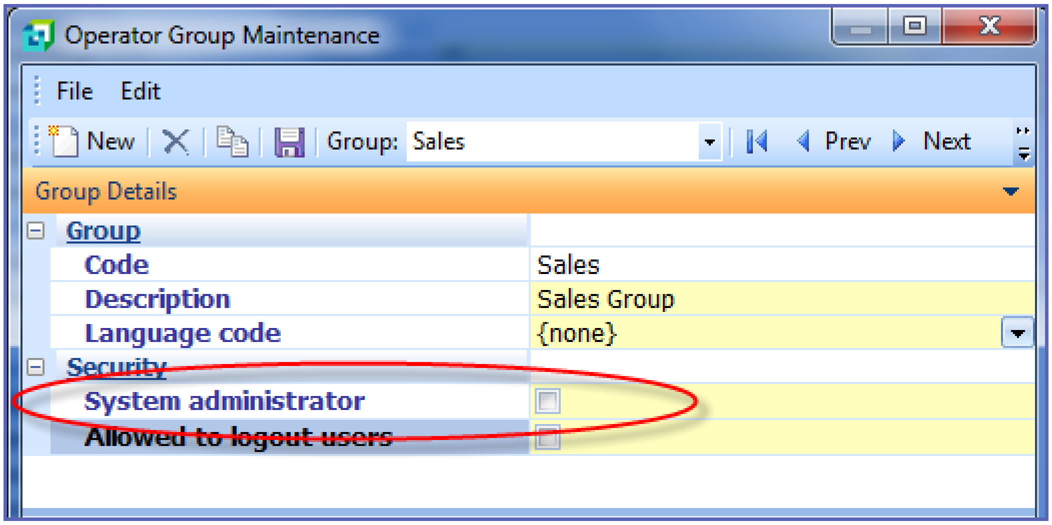
Against each individual operator code you can set whether an operator account is locked out after a number of unsuccessful login attempts.



Activities	
Selection	All
Configure activities	Edit
Fields	
Selection	All
Configure fields	Edit
Menus	
Enable standard SYSPRO menus	☑
Enable editing of user menus	☑
Enable editing of menus for same group	☑
Password	
Number of login attempts	Allow unlimited login attempts
Operator locked out	
Password never expires	
Last login	
Salesperson access control	
Assign salesperson to current operator	
Salesperson	
Apply access control	
Filter reports and browses	

Allow unlimited login attempts
Lockout after 1 failed login attempt
Lockout after 2 failed login attempts
Lockout after 3 failed login attempts
Lockout after 4 failed login attempts
Lockout after 5 failed login attempts
Lockout after 6 failed login attempts
Lockout after 7 failed login attempts
Lockout after 8 failed login attempts
Lockout after 9 failed login attempts

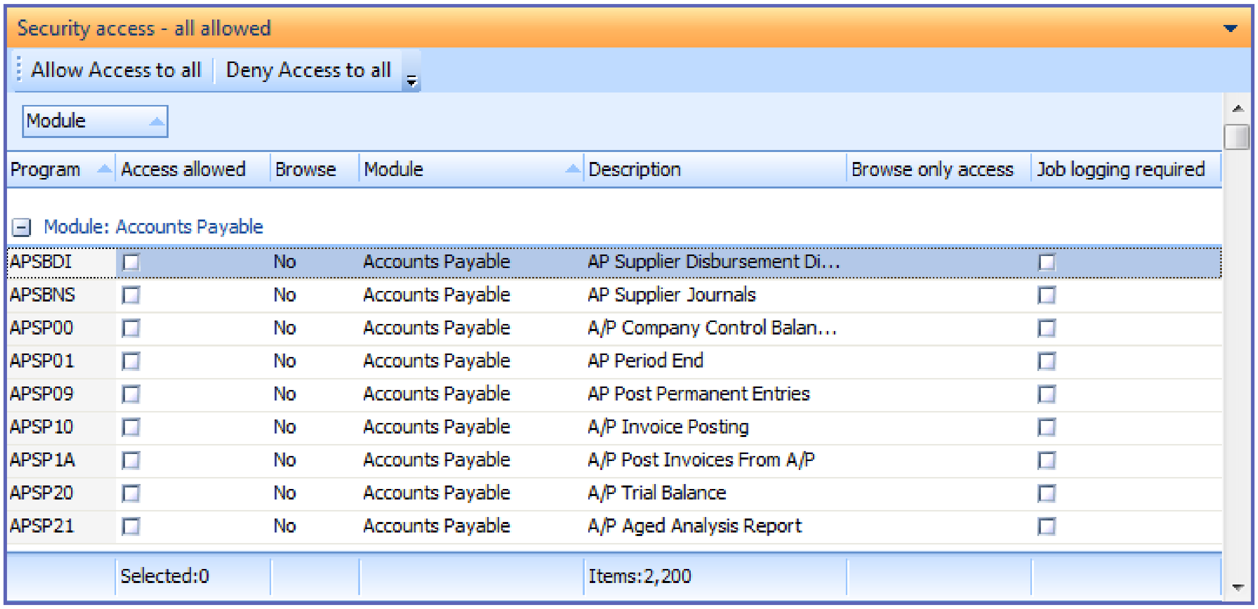
Operator codes are assigned to operator groups, and an operator group can also be defined as a "System administrator". Only the real System Administrator should belong to a group with this checkbox enabled as all operators belonging to this group can access every program throughout the system.



Group: Sales

Group	
Code	Sales
Description	Sales Group
Language code	{none}
Security	
System administrator	□
Allowed to logout users	□

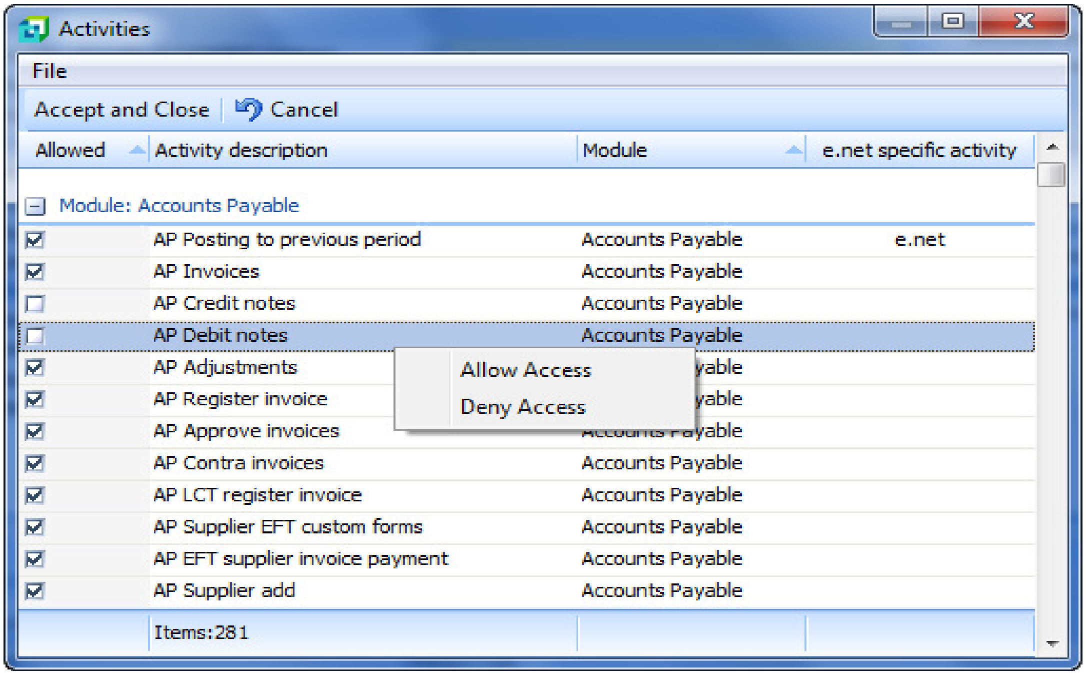
Once an operator is added to the system, it is important to ensure that they are only able to access the right programs and information. Within the Security Access section against the operator group or against the role it is possible to allow or deny access to nearly every SYSPRO program, including the e.net solutions business objects. The programs are listed under the relevant module, and e.net solutions business objects are listed under the class to which they belong.



Program	Access allowed	Browse	Module	Description	Browse only access	Job logging required
Module: Accounts Payable						
APSBDI	□	No	Accounts Payable	AP Supplier Disbursement Di...		□
APSBNS	□	No	Accounts Payable	AP Supplier Journals		□
APSP00	□	No	Accounts Payable	A/P Company Control Balan...		□
APSP01	□	No	Accounts Payable	AP Period End		□
APSP09	□	No	Accounts Payable	AP Post Permanent Entries		□
APSP10	□	No	Accounts Payable	A/P Invoice Posting		□
APSP1A	□	No	Accounts Payable	A/P Post Invoices From A/P		□
APSP20	□	No	Accounts Payable	A/P Trial Balance		□
APSP21	□	No	Accounts Payable	A/P Aged Analysis Report		□
	Selected:0			Items:2,200		

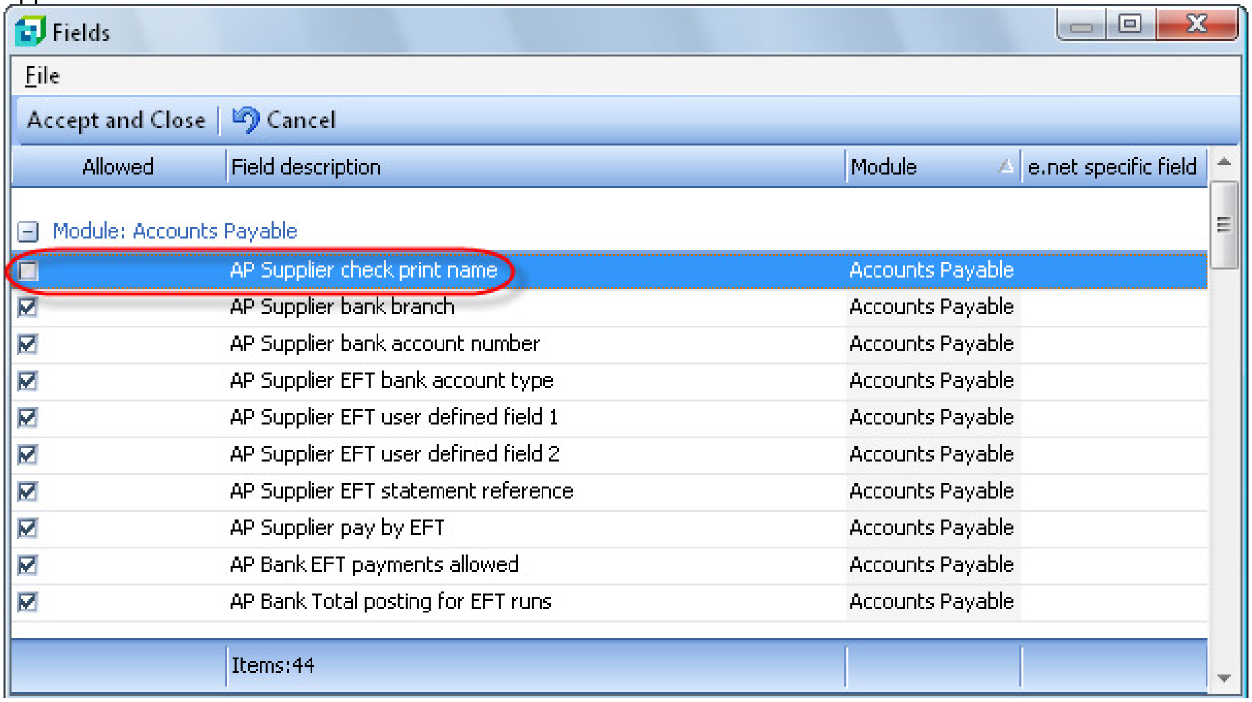
When a new operator group or role is created, you should immediately define the security access before adding operators to that role or group. You would begin by ensuring they are only able to access those programs required by the members of the group or role. The system enables you to allow or deny access to all programs or to entire modules at a click of a button. It is easier to use these settings and then selectively turn individual programs on or off. When a group or role no longer needs access to a program (or programs) because of role changes within the organization, remove this access immediately. It is unlikely that you will remember to remove it later.

Access to specific activities can be controlled at the role level or per individual operator. These activities are defined per module, for convenience.. This enables you to fine-tune what each operator or role can actually do. For example, the group or role may have access to the AP Invoice Posting program but may be prevented from posting debit or credit note activities within that program.



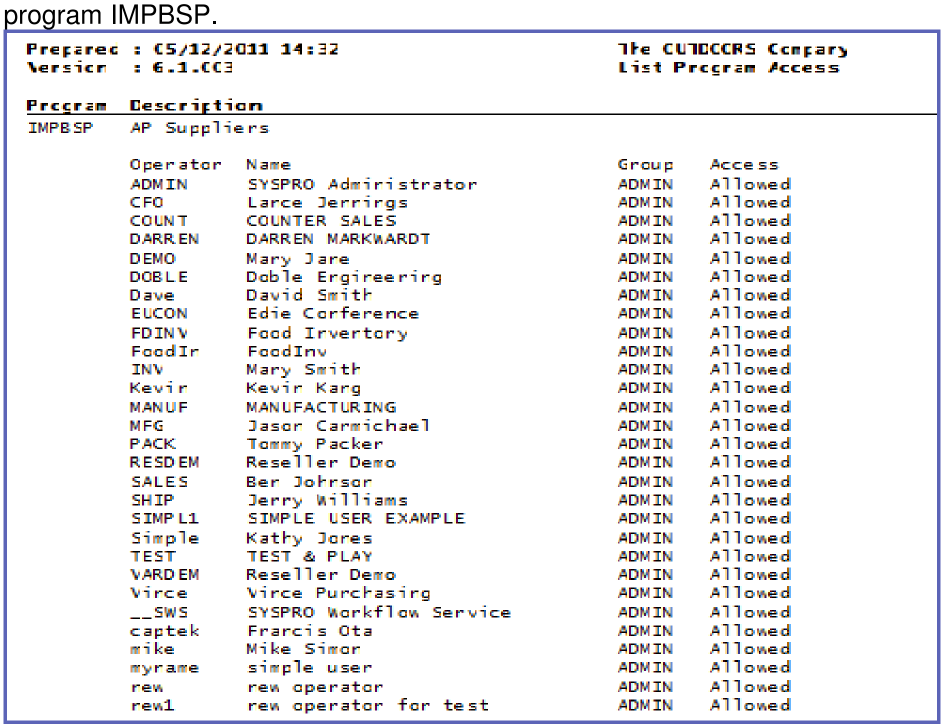
Allowed	Activity description	Module	e.net specific activity
Module: Accounts Payable			
☑	AP Posting to previous period	Accounts Payable	e.net
☑	AP Invoices	Accounts Payable	
□	AP Credit notes	Accounts Payable	
□	AP Debit notes	Accounts Payable	
☑	AP Adjustments	yable	
☑	AP Register invoice	yable	
☑	AP Approve invoices	Accounts Payable	
☑	AP Contra invoices	Accounts Payable	
☑	AP LCT register invoice	Accounts Payable	
☑	AP Supplier EFT custom forms	Accounts Payable	
☑	AP EFT supplier invoice payment	Accounts Payable	
☑	AP Supplier add	Accounts Payable	
	Items:281		

Going a step further, you can specify that operators or roles are prevented from viewing/accessing certain fields in the system. In the following example the operator is prevented from modifying the name that will appear on a check.



Allowed	Field description	Module	e.net specific field
⊟ Module: Accounts Payable			
□	AP Supplier check print name	Accounts Payable	
☑	AP Supplier bank branch	Accounts Payable	
☑	AP Supplier bank account number	Accounts Payable	
☑	AP Supplier EFT bank account type	Accounts Payable	
☑	AP Supplier EFT user defined field 1	Accounts Payable	
☑	AP Supplier EFT user defined field 2	Accounts Payable	
☑	AP Supplier EFT statement reference	Accounts Payable	
☑	AP Supplier pay by EFT	Accounts Payable	
☑	AP Bank EFT payments allowed	Accounts Payable	
☑	AP Bank Total posting for EFT runs	Accounts Payable	
	Items:44		

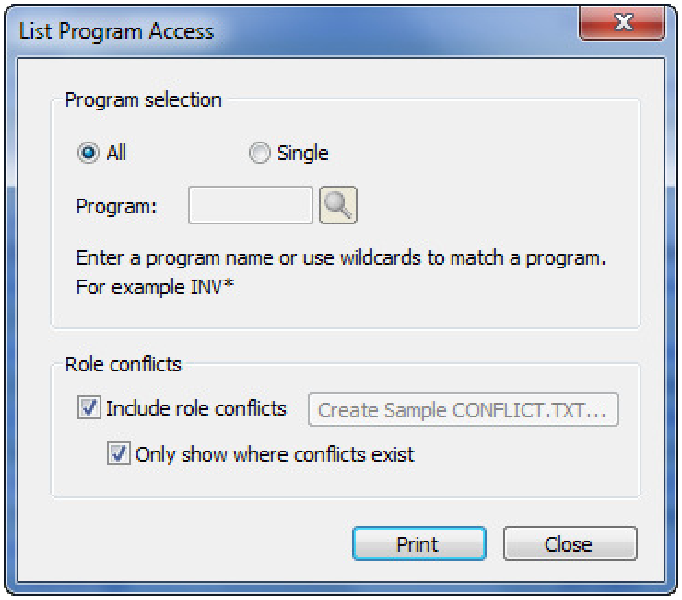
To assist you in establishing which operators can run a specific program (or range of programs, or all programs) there is a “List Program Access” report. This program is available from the browse on operator codes that appears when you call up the Operator Maintenance program. From here, select File > List Program Access. The example below is a list of all the operators that can access the Supplier browse program IMPBSP.



```
Preparec : C5/12/2011 14:32                                 The CUTDCCRS Ccrpary
Version  : 6.1.CC3                                          List Prcgram Access

Prcgram  Description
IMPBSP   AP Suppliers

         Operator  Name                                     Group    Access
         ADMIN     SYSPRO Admiristrator                     ADMIN    Allowed
         CFO       Larce Jerrirgs                           ADMIN    Allowed
         COUNT     COUNTER SALES                            ADMIN    Allowed
         DARREN    DARREN MARKWARDT                         ADMIN    Allowed
         DEMO      Mary Jare                                ADMIN    Allowed
         DOBLE     Doble Ergireerirg                        ADMIN    Allowed
         Dave      David Smith                              ADMIN    Allowed
         EUCON     Edie Corference                          ADMIN    Allowed
         FDINV     Food Irvertory                           ADMIN    Allowed
         FoodIr    FoodInv                                  ADMIN    Allowed
         INV       Mary Smith                               ADMIN    Allowed
         Kevir     Kevir Karg                               ADMIN    Allowed
         MANUF     MANUFACTURING                            ADMIN    Allowed
         MFG       Jasor Carmichael                         ADMIN    Allowed
         PACK      Tommy Packer                             ADMIN    Allowed
         RESDEM    Reseller Demo                            ADMIN    Allowed
         SALES     Ber Johrsor                              ADMIN    Allowed
         SHIP      Jerry Williams                           ADMIN    Allowed
         SIMPL1    SIMPLE USER EXAMPLE                      ADMIN    Allowed
         Simple    Kathy Jores                              ADMIN    Allowed
         TEST      TEST & PLAY                              ADMIN    Allowed
         VARDEM    Reseller Demo                            ADMIN    Allowed
         Virce     Virce Purchasirg                         ADMIN    Allowed
         __SWS     SYSPRO Workflow Service                  ADMIN    Allowed
         captek    Frarcis Ota                              ADMIN    Allowed
         mike      Mike Simor                               ADMIN    Allowed
         myrame    simple user                              ADMIN    Allowed
         rew       rew operator                             ADMIN    Allowed
         rew1      rew operator for test                    ADMIN    Allowed
```

The same program has an option to produce a Role Conflict report. This is used to highlight operators who have access to two programs that potentially allow a fraudulent activity to take place. The checking is done against a user-definable file called CONFLICT.TXT that resides in the SYSPRO work folder on the server.

The level to which the duties can be segregated is dependent on the number and quality of available staff. In smaller organizations, some staff may have to perform both sides of the transaction and some manual controls will need to be implemented. A sample CONFLICT.TXT file is provided. This template is considered to be for a "typical" company. There is an option to produce this role conflict template from within the program. If there is an existing CONFLICT.TXT file present this button will be grayed out to prevent it being overwritten.



List Program Access

Program selection

● All ○ Single

Program:

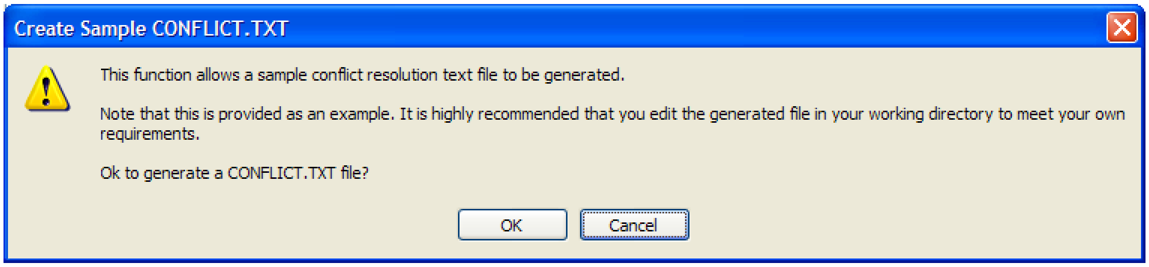
Enter a program name or use wildcards to match a program. For example INV*

Role conflicts

☑ Include role conflicts

☑ Only show where conflicts exist

If the "Create Sample CONFLICT.TXT…" button is pressed a warning message displayed stating that this is a sample and should be modified to match your requirements.



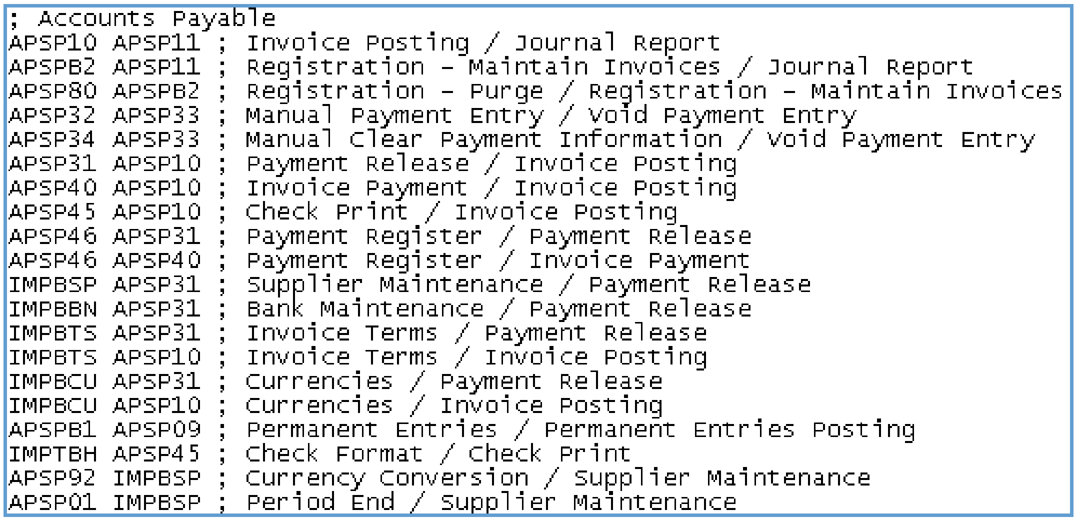
Create Sample CONFLICT.TXT

This function allows a sample conflict resolution text file to be generated.

Note that this is provided as an example. It is highly recommended that you edit the generated file in your working directory to meet your own requirements.

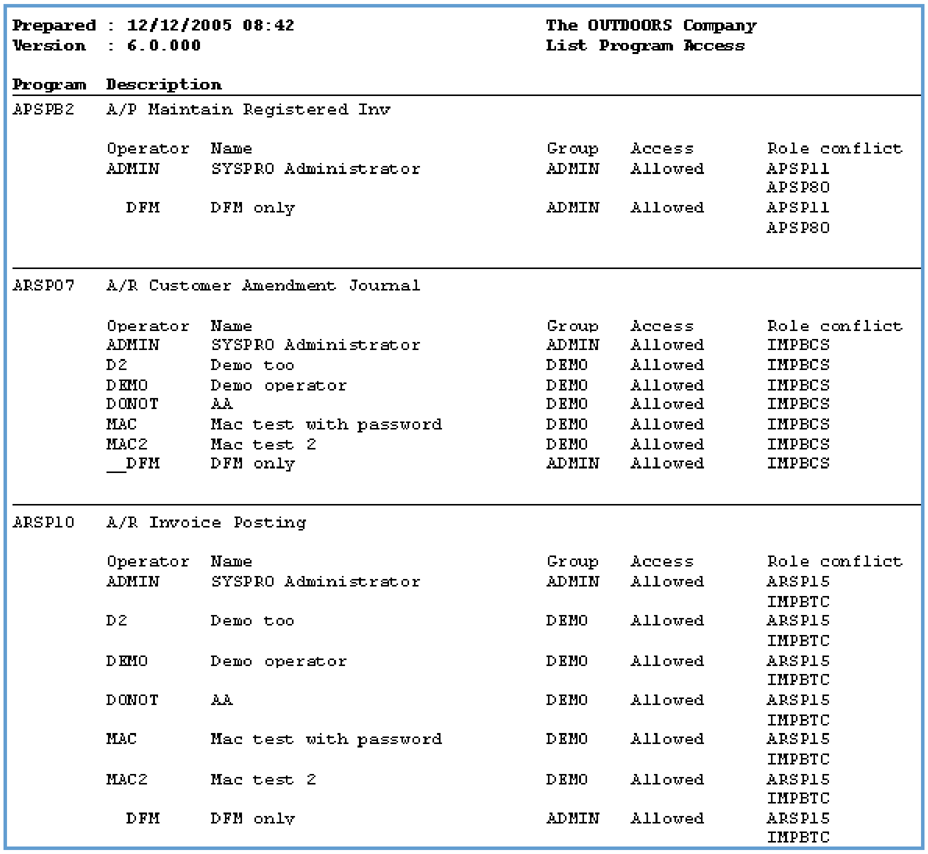
Ok to generate a CONFLICT.TXT file?

The following is a section from this sample CONFLICT.TXT file.



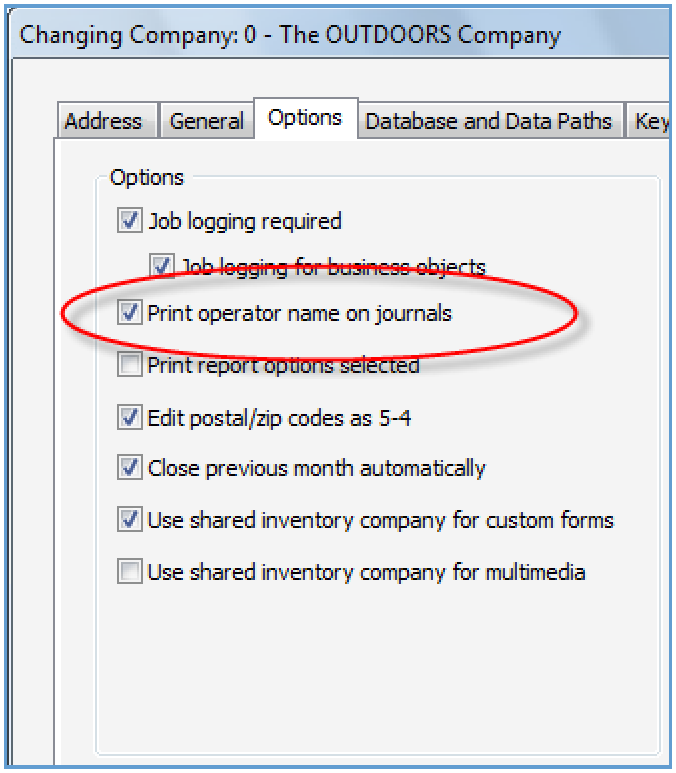
```
; Accounts Payable
APSP10 APSP11 ; Invoice Posting / Journal Report
APSPB2 APSP11 ; Registration - Maintain Invoices / Journal Report
APSP80 APSPB2 ; Registration - Purge / Registration - Maintain Invoices
APSP32 APSP33 ; Manual Payment Entry / Void Payment Entry
APSP34 APSP33 ; Manual Clear Payment Information / Void Payment Entry
APSP31 APSP10 ; Payment Release / Invoice Posting
APSP40 APSP10 ; Invoice Payment / Invoice Posting
APSP45 APSP10 ; Check Print / Invoice Posting
APSP46 APSP31 ; Payment Register / Payment Release
APSP46 APSP40 ; Payment Register / Invoice Payment
IMPBSP APSP31 ; Supplier Maintenance / Payment Release
IMPBBN APSP31 ; Bank Maintenance / Payment Release
IMPBTS APSP31 ; Invoice Terms / Payment Release
IMPBTS APSP10 ; Invoice Terms / Invoice Posting
IMPBCU APSP31 ; Currencies / Payment Release
IMPBCU APSP10 ; Currencies / Invoice Posting
APSPB1 APSP09 ; Permanent Entries / Permanent Entries Posting
IMPTBH APSP45 ; Check Format / Check Print
APSP92 IMPBSP ; Currency Conversion / Supplier Maintenance
APSP01 IMPBSP ; Period End / Supplier Maintenance
```

Following is an example of the output of a Role Conflict report. It lists, by program, which operators can run this program that can run another that may conflict with this one. In this example you can see that there is a potential conflict for some operators against ARSP07, the A/R Customer Amendment Journal report. These operators are able to modify the customer details using IMPBCS (the Customer Maintenance program) as well as print the audit trail (ARSP07). This makes it easier to hide changes made to a customer that may be changed back later.



```
Prepared : 12/12/2005 08:42                         The OUTDOORS Company
Version  : 6.0.000                                  List Program Access

Program  Description
APSPB2   A/P Maintain Registered Inv

         Operator  Name                             Group   Access       Role conflict
         ADMIN     SYSPRO Administrator             ADMIN   Allowed      APSP11
                                                                         APSP80
           DFM     DFM only                         ADMIN   Allowed      APSP11
                                                                         APSP80

ARSP07   A/R Customer Amendment Journal

         Operator  Name                             Group   Access       Role conflict
         ADMIN     SYSPRO Administrator             ADMIN   Allowed      IMPBCS
         D2        Demo too                         DEMO    Allowed      IMPBCS
         DEMO      Demo operator                    DEMO    Allowed      IMPBCS
         DONOT     AA                               DEMO    Allowed      IMPBCS
         MAC       Mac test with password           DEMO    Allowed      IMPBCS
         MAC2      Mac test 2                       DEMO    Allowed      IMPBCS
         __DFM     DFM only                         ADMIN   Allowed      IMPBCS

ARSP10   A/R Invoice Posting

         Operator  Name                             Group   Access       Role conflict
         ADMIN     SYSPRO Administrator             ADMIN   Allowed      ARSP15
                                                                         IMPBTC
         D2        Demo too                         DEMO    Allowed      ARSP15
                                                                         IMPBTC
         DEMO      Demo operator                    DEMO    Allowed      ARSP15
                                                                         IMPBTC
         DONOT     AA                               DEMO    Allowed      ARSP15
                                                                         IMPBTC
         MAC       Mac test with password           DEMO    Allowed      ARSP15
                                                                         IMPBTC
         MAC2      Mac test 2                       DEMO    Allowed      ARSP15
                                                                         IMPBTC
           DFM     DFM only                         ADMIN   Allowed      ARSP15
                                                                         IMPBTC
```

It is also useful to print the name of the operator who performed the task on audit trails. This avoids you having to manually look up which operator code performed the task and then cross reference this to an operator name at a later time. Within the configuration options for the company, you can specify that the operator name will be printed on journals.


Changing Company: 0 - The OUTDOORS Company

Options

☑ Job logging required

☑ Job logging for business objects

☑ Print operator name on journals

□ Print report options selected

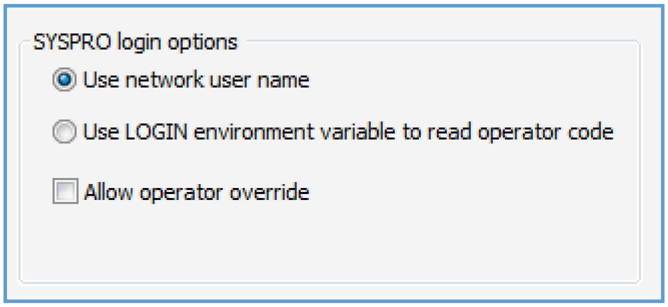
☑ Edit postal/zip codes as 5-4

☑ Close previous month automatically

☑ Use shared inventory company for custom forms

□ Use shared inventory company for multimedia

In the System Setup program, there is an option to default the operator login code to the same one used to login to the network. This can be useful, providing that the operator codes are the same for both SYSPRO and the operating system. In addition, there is an option to prevent the operator from overriding this default operator code. By doing this, you prevent other operators from logging in as their colleagues unless they are able to login to the operating system as them too.

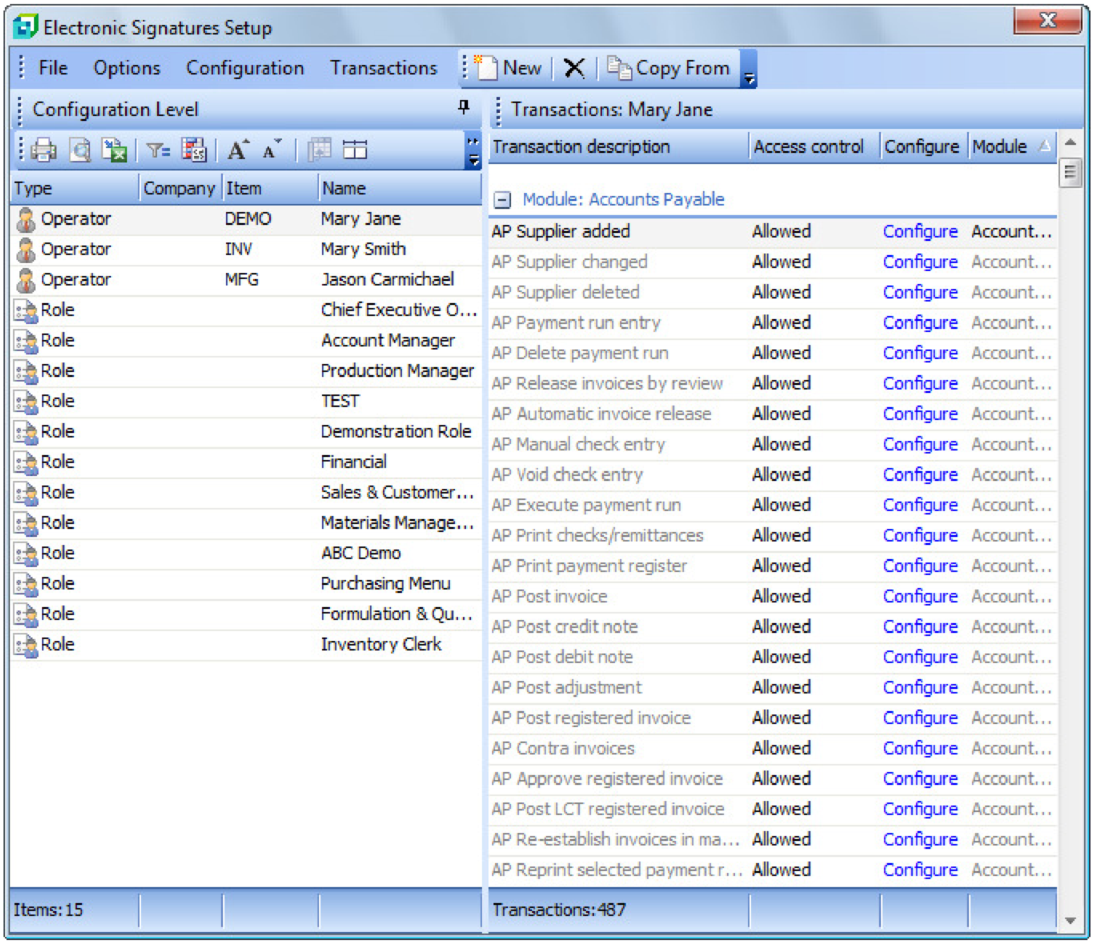

SYSPRO login options

● Use network user name

○ Use LOGIN environment variable to read operator code

□ Allow operator override

SYSPRO's Electronic Signature system offers an additional level of security whereby the System Administrator can control areas of their enterprise system to prevent unauthorized activities from occurring, control who performs these activities, and monitor these via audit logs.



Type	Company	Item	Name
Operator		DEMO	Mary Jane
Operator		INV	Mary Smith
Operator		MFG	Jason Carmichael
Role			Chief Executive O...
Role			Account Manager
Role			Production Manager
Role			TEST
Role			Demonstration Role
Role			Financial
Role			Sales & Customer...
Role			Materials Manage...
Role			ABC Demo
Role			Purchasing Menu
Role			Formulation & Qu...
Role			Inventory Clerk

Items: 15

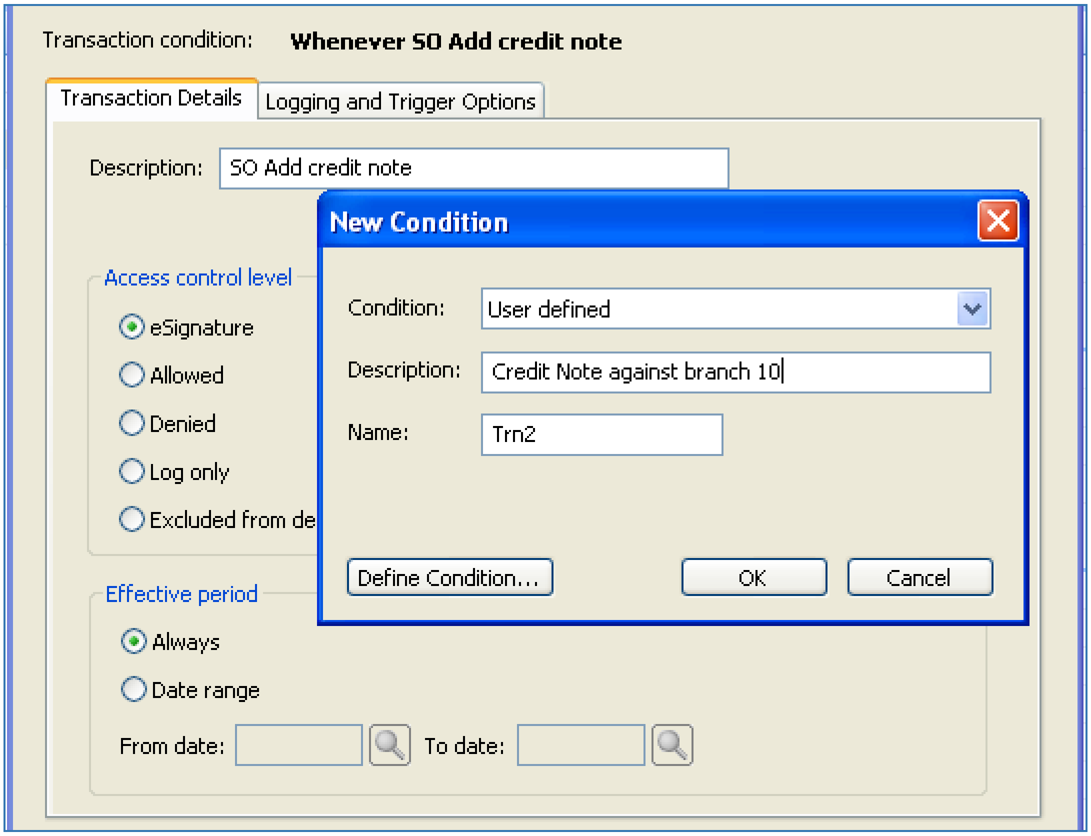
Transaction description	Access control	Configure	Module
Module: Accounts Payable			
AP Supplier added	Allowed	Configure	Account...
AP Supplier changed	Allowed	Configure	Account...
AP Supplier deleted	Allowed	Configure	Account...
AP Payment run entry	Allowed	Configure	Account...
AP Delete payment run	Allowed	Configure	Account...
AP Release invoices by review	Allowed	Configure	Account...
AP Automatic invoice release	Allowed	Configure	Account...
AP Manual check entry	Allowed	Configure	Account...
AP Void check entry	Allowed	Configure	Account...
AP Execute payment run	Allowed	Configure	Account...
AP Print checks/remittances	Allowed	Configure	Account...
AP Print payment register	Allowed	Configure	Account...
AP Post invoice	Allowed	Configure	Account...
AP Post credit note	Allowed	Configure	Account...
AP Post debit note	Allowed	Configure	Account...
AP Post adjustment	Allowed	Configure	Account...
AP Post registered invoice	Allowed	Configure	Account...
AP Contra invoices	Allowed	Configure	Account...
AP Approve registered invoice	Allowed	Configure	Account...
AP Post LCT registered invoice	Allowed	Configure	Account...
AP Re-establish invoices in ma...	Allowed	Configure	Account...
AP Reprint selected payment r...	Allowed	Configure	Account...

Transactions: 487

The e-Signature system enables the system administrator to identify key business processes that need additional control, and flag them as being under the control of the e-Signature system.

Multiple conditions can be configured against each business process for the whole system, per operator group, per role or by operator. For example, one business process might be when a credit note is processed. The conditions might be based on the branch code against which the credit note is being apllied so that different people in the organization are notified accordingly. Against each condition it is possible to set a security level. The operator (or operator group or system wide) can be set to either require a password and log the activity, just log the activity, deny access to this condition, or not be set for this condition.

It is also possible to set a date range for which these security levels are required.



Transaction condition: **Whenever SO Add credit note**

Description: SO Add credit note

Access control level

● eSignature
○ Allowed
○ Denied
○ Log only
○ Excluded from de

Effective period

● Always
○ Date range

From date: To date:

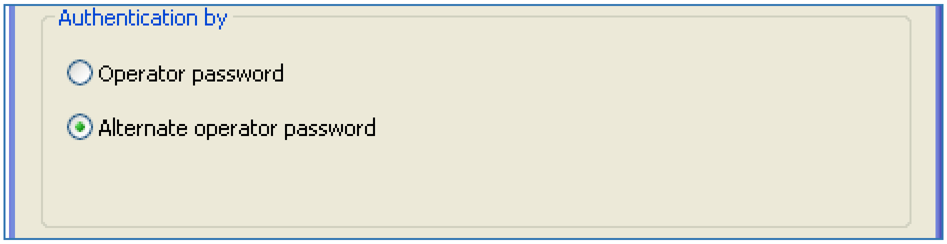
New Condition

Condition: User defined

Description: Credit Note against branch 10

Name: Trn2

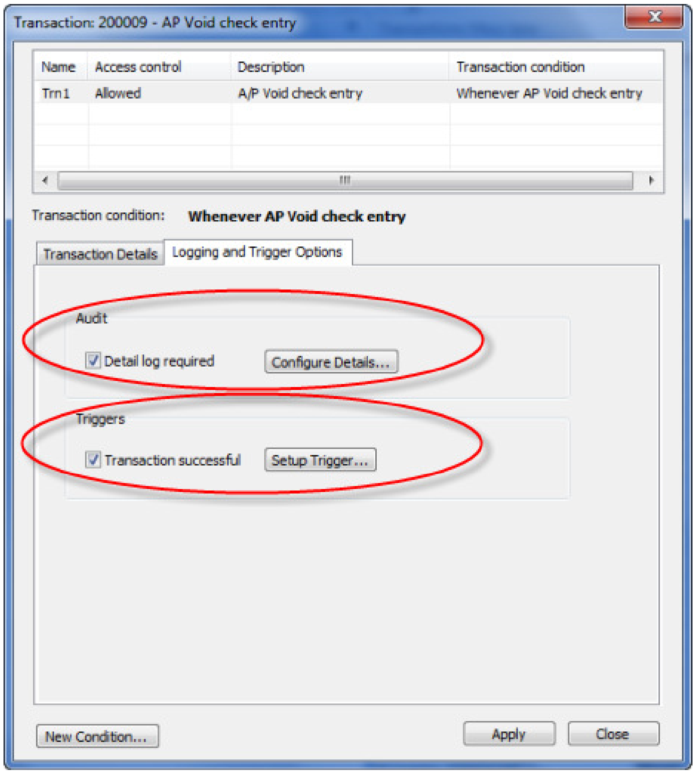
The password required by the e-Signature system could be the same password the operator uses to login to SYSPRO, or an alternate operator password could be defined. This password would then be used to authenticate the operator when required by the e-Signature system.



Authentication by

○ Operator password
● Alternate operator password

In addition, you can configure the e-Signature system to activate triggers for integration to third-party systems or notification via email, as well as maintain a detailed transaction log for auditing purposes. The transaction log can be retained indefinitely.

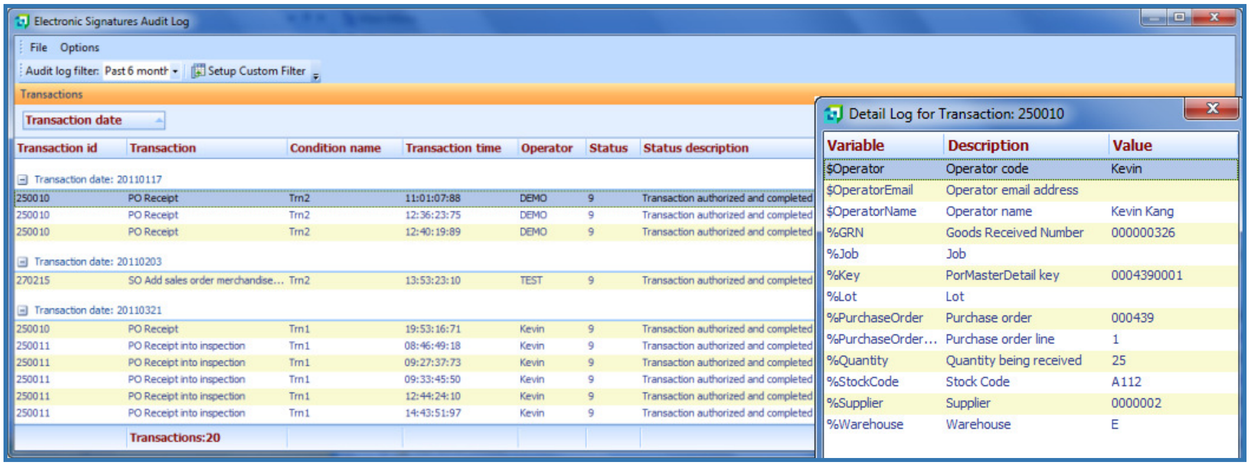


Transaction: 200009 - AP Void check entry

Name	Access control	Description	Transaction condition
Trn1	Allowed	A/P Void check entry	Whenever AP Void check entry

Transaction condition: **Whenever AP Void check entry**

The audit log can be viewed and printed by an Administrator to see who authorized each transaction and exactly when it occurred, and view the details of the transaction. A configuration option will allow definition of how long the audit log is to be retained – including an option to retain it indefinitely. Only the System Administrator will be able to purge the audit log and a record of this will be stored in the job logging system.



Electronic Signatures Audit Log

Transaction id	Transaction	Condition name	Transaction time	Operator	Status	Status description
Transaction date: 20110117						
250010	PO Receipt	Trn2	11:01:07:88	DEMO	9	Transaction authorized and completed
250010	PO Receipt	Trn2	12:36:23:75	DEMO	9	Transaction authorized and completed
250010	PO Receipt	Trn2	12:40:19:89	DEMO	9	Transaction authorized and completed
Transaction date: 20110203						
270215	SO Add sales order merchandise...	Trn2	13:53:23:10	TEST	9	Transaction authorized and completed
Transaction date: 20110321						
250010	PO Receipt	Trn1	19:53:16:71	Kevin	9	Transaction authorized and completed
250011	PO Receipt into inspection	Trn1	08:46:49:18	Kevin	9	Transaction authorized and completed
250011	PO Receipt into inspection	Trn1	09:27:37:73	Kevin	9	Transaction authorized and completed
250011	PO Receipt into inspection	Trn1	09:33:45:50	Kevin	9	Transaction authorized and completed
250011	PO Receipt into inspection	Trn1	12:44:24:10	Kevin	9	Transaction authorized and completed
250011	PO Receipt into inspection	Trn1	14:43:51:97	Kevin	9	Transaction authorized and completed
	Transactions:20					

Detail Log for Transaction: 250010

Variable	Description	Value
$Operator	Operator code	Kevin
$OperatorEmail	Operator email address	
$OperatorName	Operator name	Kevin Kang
%GRN	Goods Received Number	000000326
%Job	Job	
%Key	PorMasterDetail key	0004390001
%Lot	Lot	
%PurchaseOrder	Purchase order	000439
%PurchaseOrder...	Purchase order line	1
%Quantity	Quantity being received	25
%StockCode	Stock Code	A112
%Supplier	Supplier	0000002
%Warehouse	Warehouse	E

The Job Logging program maintains a log file of all programs that have been accessed by operators and can be used together with the System Audit log to more effectively manage system security.

Integrity of Operations

Controls for change management

It is important that a company's processes are documented, validated and adhered to. SYSPRO provides a business process management solution, SYSPRO Process Modeling (SPM) that enables companies to produce a blueprint of their business. SPM starts at the high level processes and goes down to the data entry level within each required program. This is the ideal tool to use when implementing SYSPRO, as it allows the implementing company to visualize their solution, buy into the project and transition more easily and willingly to a new software product. It also highlights areas that require security and validates their compliancy.

This is also an ideal tool for existing SYSPRO companies looking to improve their processes and ensure they are meeting the regulations required by their industry or government. SPM can be implemented at any stage of the SYSPRO life cycle. It should also be used when new processes are implemented or when processes require change (which may require additional software) to obtain confirmation and endorsement from management.

New employees or existing employees moving to a new position can quickly and easily understand their job function and how it fits into the organization.

SYSPRO Workflow Services can also be used to automate steps in processes and force acceptance or rejection of information before proceeding to the next step.

Having the ability to document, visualize and automate processes offers a level of security and comfort for management having to authorize change.

Business processes should be reviewed on a regular basis to ensure that the process that is being executed is the one that the company believes is happening.

Controls for software updates

This relates to both updates of the SYSPRO product and any software add-ons or custom development around the product. For updates to the SYSPRO product we recommend that you have a test server and a live server. Any changes to SYSPRO (such as a new version or release, weekly port, hot fixes, configuration option or procedural changes) are first loaded onto the test server. Tests are performed and when the person performing the tests is satisfied with these changes they are signed off and deployed to the live server. SYSPRO provides the ability for customers who have stringent change control procedures in place to selectively manage their updates through "fix packs" targeted at a specific error correction.

Similar steps are taken for custom development or add-ons to the core SYSPRO product. It is often recommended that a development environment is completely isolated if possible i.e. instead of just having a Live and Test server in this environment, that there is also a Development server. The developers should never have access to the Live server, and if there are three servers it is recommended that they do not access the Test server either. Development should be done on the Development server or in an isolated environment. When development want the change tested, it is packaged and passed to the testers, who load it on to the Test server. When they are satisfied with the software, they sign it off and it is deployed to the Live server.

Changes and enhancements to SYSPRO are documented and made available on SYSPRO's Support Zone. These documents should be downloaded and copies kept on site (see the following section for more information).

It is also recommended that someone other than the system administrator review system setup changes, as well as review the system audit log as this will highlight key system changes/occurrences that the company should be aware of.

Understanding key system configurations

Over time, software products such as SYSPRO improve in functionality and features. Many new features, functions and configuration options are added, along with additional modules. Operators and system administrators leave the organization and are replaced. Sometimes they are replaced from within the organization, in which case knowledge is passed on from the outgoing personnel. Research has shown that each time this information is passed on, a significant amount of this knowledge is lost, in many cases, up to 20%. So if, for example, you are on your 3rd system administrator since the original training, and the original system administrator remembered everything they were taught, the latest administrator will have less than 65% of the original knowledge. It is also human nature to only remember things that are important, and that are used regularly. So, if an area of the product training has not been used for a significant length of time, it will also be forgotten.

It is therefore important for existing administrators and operators to attend refresher training. This can be tied into the release of a new release or issue of SYSPRO. New operators, and especially administrators, should attend training as a matter of course.

Administrators should also review the list of enhancements on the SYSPRO Support Zone (System administrator should all have access to the SYSPRO Support Zone. If they do not, they should request it by completing the online form. Access is free to SYSPRO customers and VARs).

For each SYSPRO version/issue there is a list of enhancements that have been added to the product. By reviewing the version/issue that you are on you will familiarize yourself with all the new functionality that it contains. This is presented by port number and contains detailed information on the enhancement. The "Site updates" section of the Support Zone contains a list of updates to the site so that there is one place to check on any changes. Updates are shown by month.

The SYSPRO Help is also a good place to find out about configuration options, as well as your SYSPRO VAR. Information about new functionality is usually recorded in higher-level overview type sessions as well as shorter feature specific viewlets/mini recordings; these all made available via the Support Zone.

SYSPRO also provides STARS (Structured Technique to Achieve a Rapid Solution) which is a methodology to guide implementers in all aspects of the implementation process, and provides a framework by which business practices can be examined and re-energized to maximize overall operational efficiency.

Auditability

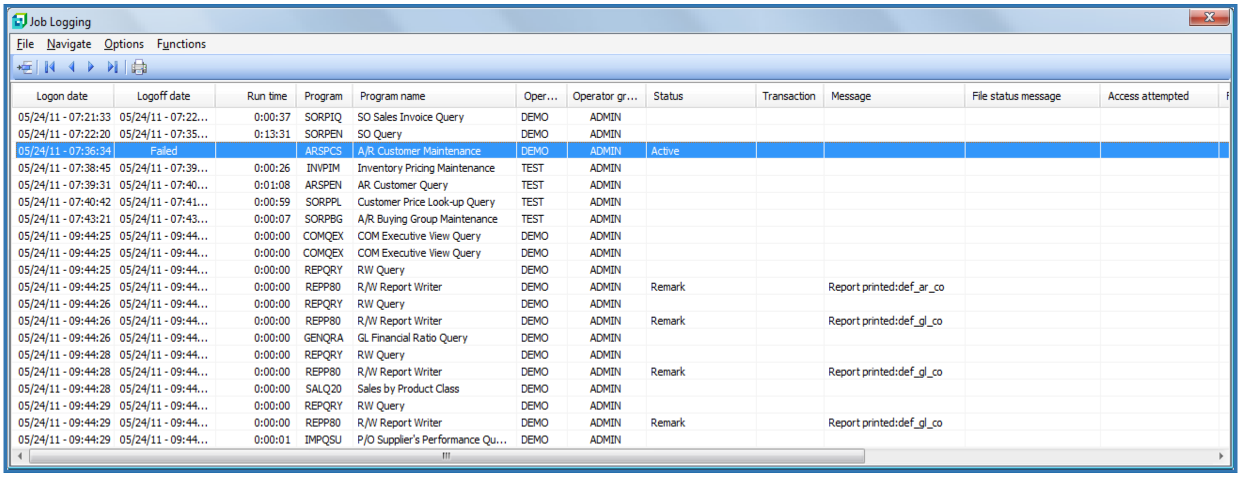
Reviewing audit logs

Journals, registers, job logging and many other documents are available from within SYSPRO as audit trails of what has happened on your system. These need to be produced and reviewed regularly. If you save up all your journals and print them only at the end of the month it is unlikely that you will review them properly.

With Sarbanes-Oxley, it is not just a case of reviewing these documents; you must prove that this was done. It is therefore recommended that these reports are scheduled to be produced using the SYSPRO Reporting Services and automatically delivered to the appropriate parties electronically. Companies could make use SYSPRO Workflow Services to obtain electronic signoff as audit trails are reviewed.

There are also many operating system audit logs that should be reviewed regularly:

- **Job Logging**
  The job logging facility keeps track of each program that was run, who ran it, the date/time it was started, the date/time it finished, how long it took and any error messages that were encountered.

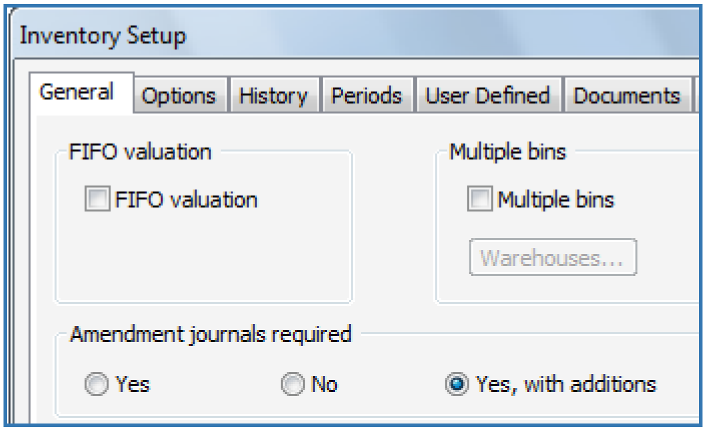


Logon date	Logoff date	Run time	Program	Program name	Oper...	Operator gr...	Status	Transaction	Message	File status message	Access attempted
05/24/11 - 07:21:33	05/24/11 - 07:22...	0:00:37	SORPIQ	SO Sales Invoice Query	DEMO	ADMIN					
05/24/11 - 07:22:20	05/24/11 - 07:35...	0:13:31	SORPEN	SO Query	DEMO	ADMIN					
05/24/11 - 07:36:34	Failed		ARSPCS	A/R Customer Maintenance	DEMO	ADMIN	Active				
05/24/11 - 07:38:45	05/24/11 - 07:39...	0:00:26	INVPIM	Inventory Pricing Maintenance	TEST	ADMIN					
05/24/11 - 07:39:31	05/24/11 - 07:40...	0:01:08	ARSPEN	AR Customer Query	TEST	ADMIN					
05/24/11 - 07:40:42	05/24/11 - 07:41...	0:00:59	SORPPL	Customer Price Look-up Query	TEST	ADMIN					
05/24/11 - 07:43:21	05/24/11 - 07:43...	0:00:07	SORPBG	A/R Buying Group Maintenance	TEST	ADMIN					
05/24/11 - 09:44:25	05/24/11 - 09:44...	0:00:00	COMQEX	COM Executive View Query	DEMO	ADMIN					
05/24/11 - 09:44:25	05/24/11 - 09:44...	0:00:00	COMQEX	COM Executive View Query	DEMO	ADMIN					
05/24/11 - 09:44:25	05/24/11 - 09:44...	0:00:00	REPQRY	RW Query	DEMO	ADMIN					
05/24/11 - 09:44:25	05/24/11 - 09:44...	0:00:00	REPP80	R/W Report Writer	DEMO	ADMIN	Remark		Report printed:def_ar_co		
05/24/11 - 09:44:26	05/24/11 - 09:44...	0:00:00	REPQRY	RW Query	DEMO	ADMIN					
05/24/11 - 09:44:26	05/24/11 - 09:44...	0:00:00	REPP80	R/W Report Writer	DEMO	ADMIN	Remark		Report printed:def_gl_co		
05/24/11 - 09:44:26	05/24/11 - 09:44...	0:00:00	GENQRA	GL Financial Ratio Query	DEMO	ADMIN					
05/24/11 - 09:44:28	05/24/11 - 09:44...	0:00:00	REPQRY	RW Query	DEMO	ADMIN					
05/24/11 - 09:44:28	05/24/11 - 09:44...	0:00:00	REPP80	R/W Report Writer	DEMO	ADMIN	Remark		Report printed:def_gl_co		
05/24/11 - 09:44:28	05/24/11 - 09:44...	0:00:00	SALQ20	Sales by Product Class	DEMO	ADMIN					
05/24/11 - 09:44:29	05/24/11 - 09:44...	0:00:00	REPQRY	RW Query	DEMO	ADMIN					
05/24/11 - 09:44:29	05/24/11 - 09:44...	0:00:00	REPP80	R/W Report Writer	DEMO	ADMIN	Remark		Report printed:def_gl_co		
05/24/11 - 09:44:29	05/24/11 - 09:44...	0:00:01	IMPQSU	P/O Supplier's Performance Qu...	DEMO	ADMIN					

  It is possible to reduce the amount of information displayed by configuring the display options. You can select to only display entries with file errors, those that are still active, those with remarks against them, transactions that were rolled back, those that failed, only entries for a specific operator, program or date range. The Administrator can print these logs for auditing purposes.

- **Journal Reports and Registers**
  All transaction posting programs such as Inventory Movements, Accounts Receivable Invoice Posting, WIP issues and receipts, etc., produce audit trails (journal reports/registers) that represent the information posted to the general ledger module to produce the company's financials. You can specify how long each of these files should be retained. Once they reach this age, they are removed the next time the relevant purge is run, provided that they have been printed. If they have not been printed, they will not be purged.

- **Amendment Journals**
  All programs that maintain key static information for each module (e.g. Stock Code Setup for Inventory control, Customer Setup for Accounts Receivable, etc.) have options to create amendment journals. Depending on the selection, these keep track of changes to these primary items, as well as items being added. The example below is from the Inventory Setup program and specifies whether amendment journals should be retained for stock codes, and whether new items should be included in the journal report.



Inventory Setup

FIFO valuation

□ FIFO valuation

Multiple bins

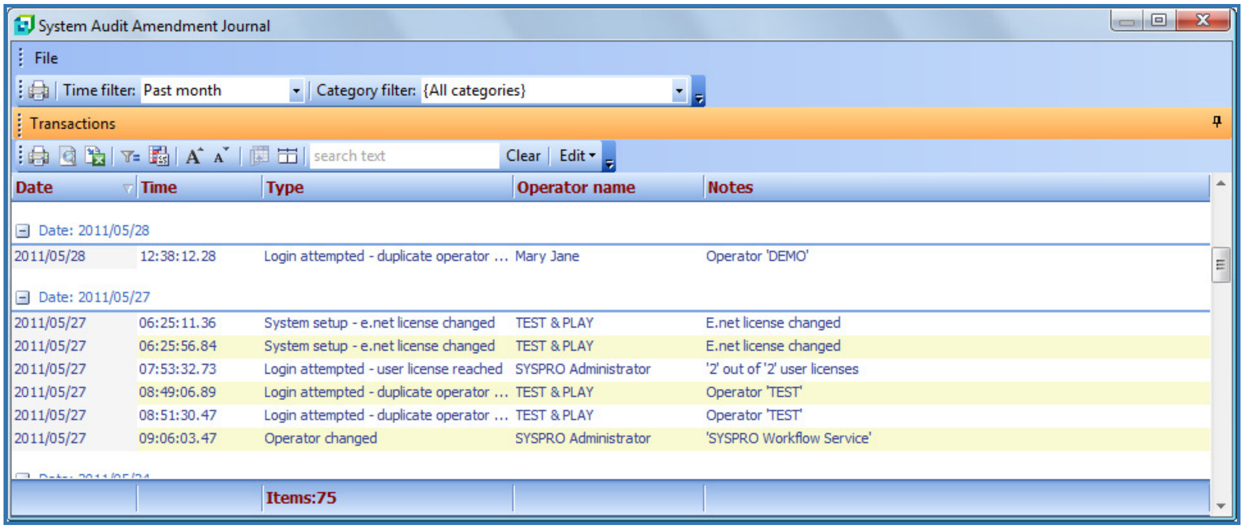
□ Multiple bins

Amendment journals required

○ Yes ○ No ● Yes, with additions

- **Setup Amendment Jornals**
  An amendment journal/audit trail is also retained of changes made to the setup/configuration options for each module, as well as the Company Setup options and Registration information. This includes date/time, operator, program name, which tab the option is on, the option value before and after, and which operator made the change.

- **System Audit log**
  Additionally, the System Audit log program allows the Administrator to manage the systems security more effectively by automatically creating a log of changes or events which occurred in the system that could affect system integrity. The transaction logs can optionally be printed and they can be purged using the System Audit Log Purge program. This log includes password changes, attempted logins, changes to roles, groups and operators, changes to system or company setup information, and indicates if the supervisor used or changed the overriding password. It is important that this log be sent to both the SYSPRO supevisor as well as the CFO of the company.



System Audit Amendment Journal

Time filter: Past month

Category filter: {All categories}

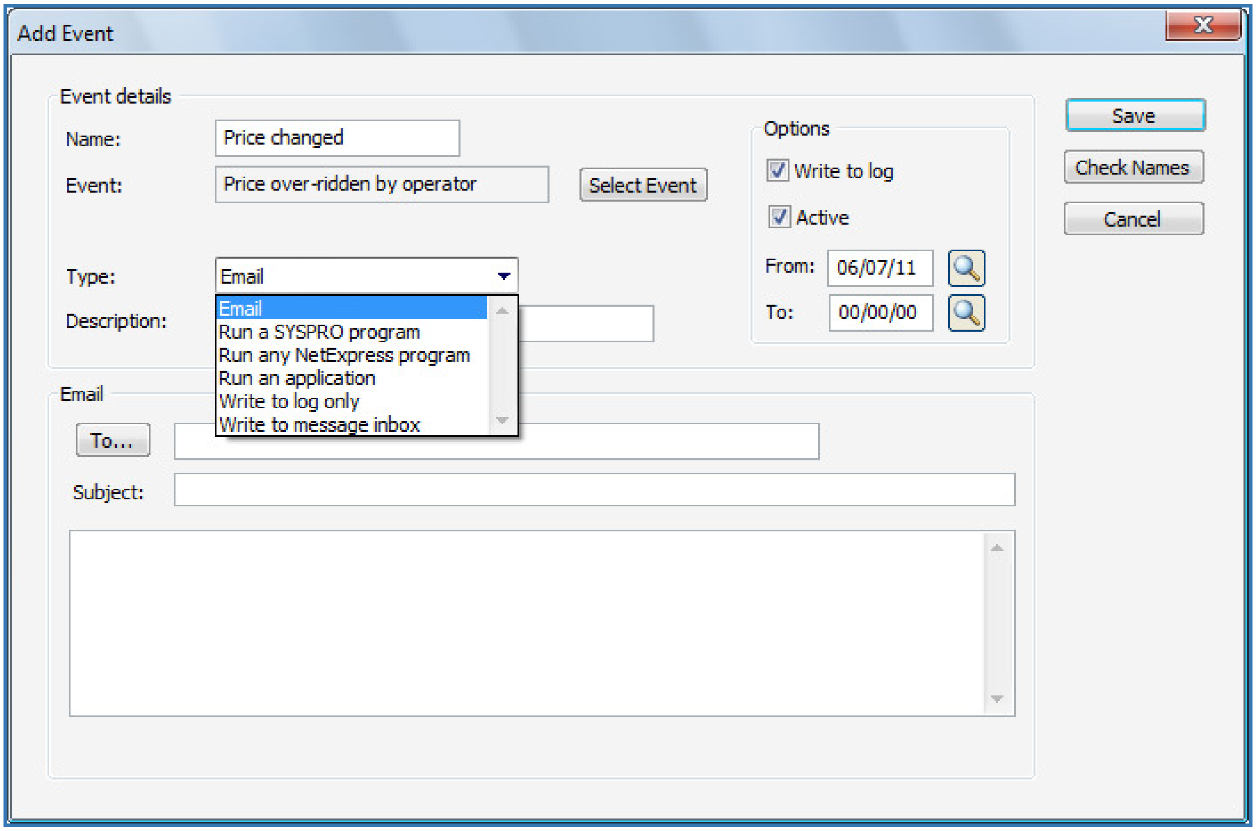
Date	Time	Type	Operator name	Notes
Date: 2011/05/28				
2011/05/28	12:38:12.28	Login attempted - duplicate operator ...	Mary Jane	Operator 'DEMO'
Date: 2011/05/27				
2011/05/27	06:25:11.36	System setup - e.net license changed	TEST & PLAY	E.net license changed
2011/05/27	06:25:56.84	System setup - e.net license changed	TEST & PLAY	E.net license changed
2011/05/27	07:53:32.73	Login attempted - user license reached	SYSPRO Administrator	'2' out of '2' user licenses
2011/05/27	08:49:06.89	Login attempted - duplicate operator ...	TEST & PLAY	Operator 'TEST'
2011/05/27	08:51:30.47	Login attempted - duplicate operator ...	TEST & PLAY	Operator 'TEST'
2011/05/27	09:06:03.47	Operator changed	SYSPRO Administrator	'SYSPRO Workflow Service'
		Items:75		

One area that will require manual documentation is if you have Report Writer reports that modify data and write back to the data files/tables. This documentation needs to state exactly what the report does, when changes were made to it and what these changes were. It is recommended that these types of reports are password protected so that they are only run by authorized personnel.

Identifying abnormal transactions in a timely manner

Printing and reviewing audit trails will help detect abnormal transactions, but the person performing the review must be observant.
SYSPRO has built-in mechanisms to warn when particular activities occur, or when pre-defined limits have been reached; the Event Management System performs checks on the server for changes, the Trigger System fires as it makes changes, and Desktop Alerts can be a combination of both parameters

Events can be configured to send e-mails, run another SYSPRO program, run a custom-written NetExpress program, run another application, write to a log file or write to the message inbox. There are many variables that can be used to pass meaningful information to the application or e-mail.



Add Event

Event details

Name: Price changed

Event: Price over-ridden by operator

Type: Email

Description:

Options

☑ Write to log

☑ Active

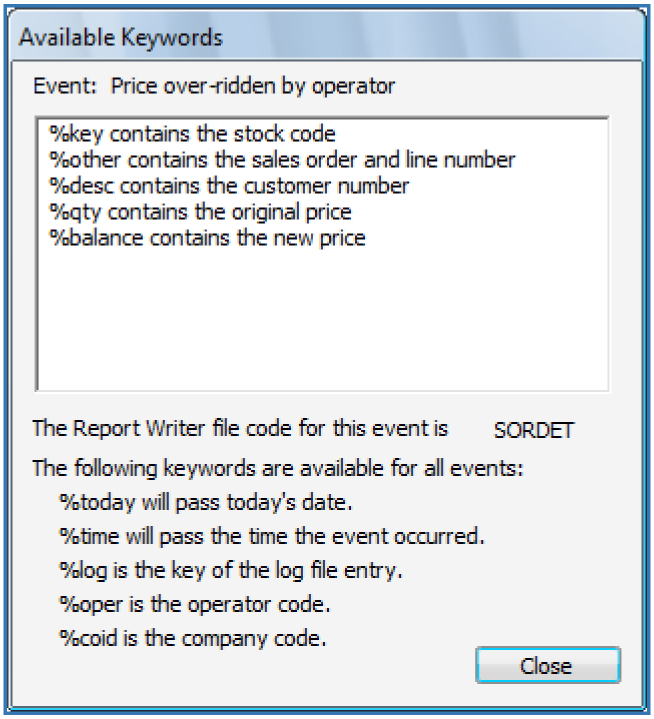
From: 06/07/11

To: 00/00/00

Email

Subject:

An example of an event that can warn you of an abnormal transaction is the Sales Order Entry and Maintenance one that fires if the operator overrides the price. Below is a list of variables that can be used in the email/message application.



Event: Price over-ridden by operator

%key contains the stock code
%other contains the sales order and line number
%desc contains the customer number
%qty contains the original price
%balance contains the new price

The Report Writer file code for this event is SORDET

The following keywords are available for all events:

%today will pass today's date.
%time will pass the time the event occurred.
%log is the key of the log file entry.
%oper is the operator code.
%coid is the company code.

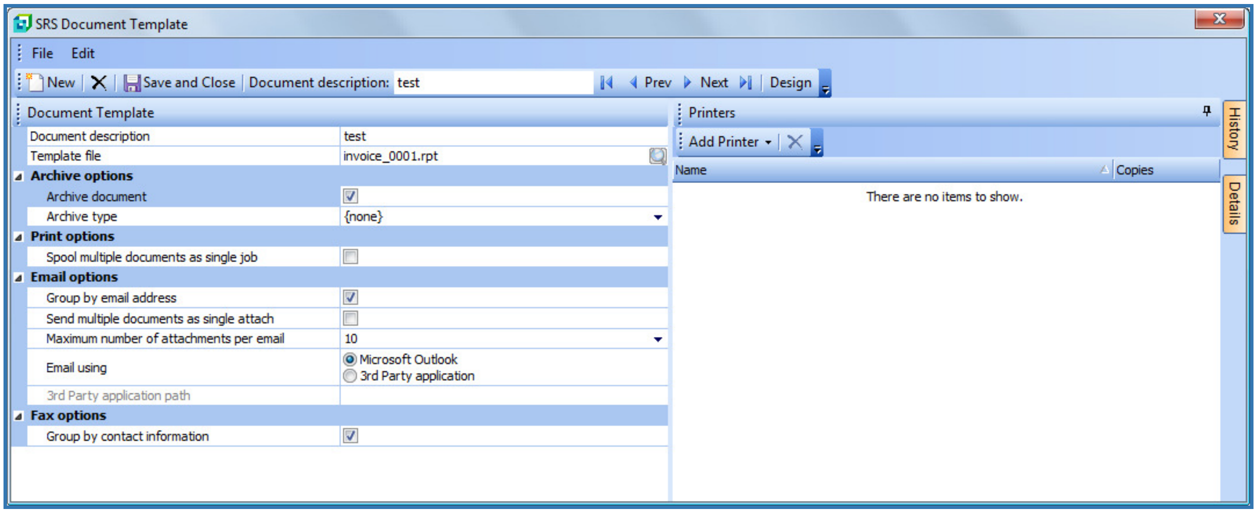
There are many events available; too many to list here. Two particularly useful ones are under the System Admin section. These are when a user receives a 'File in use' error and when there is an 'Access security breach attempt'.

Triggers are slightly different to events in that they happen on the client as the transaction is processed. There are several that can be used to highlight potentially abnormal transactions. Some examples are when an Accounts Payable check is voided, after an Assets Register asset is revalued or after an EFT beneficiary has been changed. These transactions in themselves are not cause for concern, but are some of the ways that fraud can occur.

Electronic signatures can also be used to highlight anomalies. Although electronic signatures is designed to authenticate operators performing specific transactions, this feature can be also used to trigger an event, email a notification or merely log the transaction as a result of a specified condition, without actually requesting operator authentication.

Archiving and retrieval of reports and documents

Sarbanes-Oxley requires organizations to have adequate internal control to manage electronic record retrieval such as financial reports and document management for a period of five years. Companies are prohibited from altering, destroying, mutilating, concealing, covering up or falsifying records. The legislation requires companies to protect and safeguard business records, to have reliable records management practices and be able to retain and retrieve data efficiently



SRS Document Template
File Edit
New | Save and Close | Document description: test | Prev | Next | Design
Printers
Add Printer
History
Details

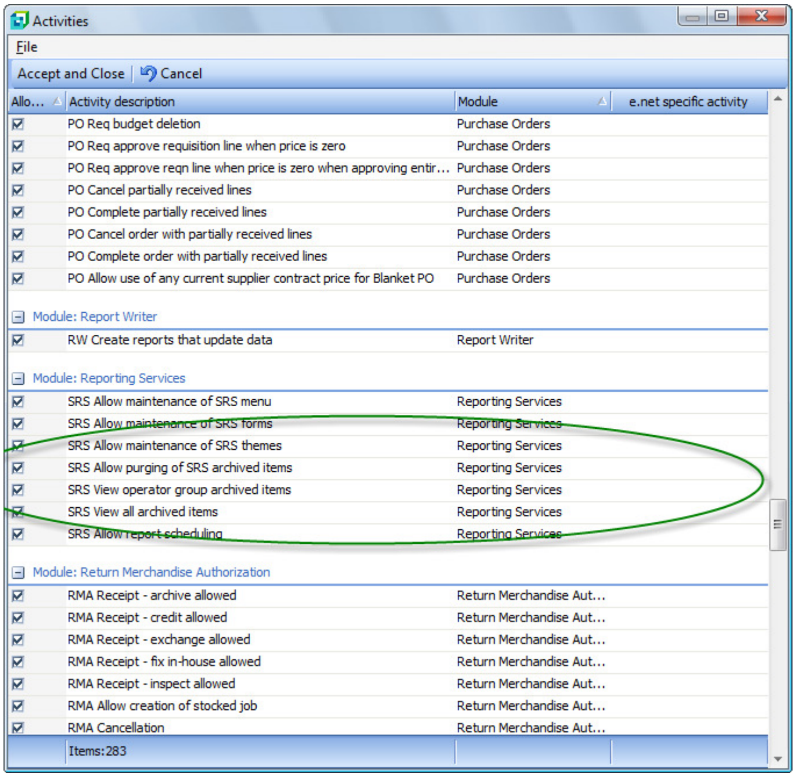
Document Template

Document description	test
Template file	invoice_0001.rpt
Archive options	
Archive document	☑
Archive type	{none}
Print options	
Spool multiple documents as single job	□
Email options	
Group by email address	☑
Send multiple documents as single attach	□
Maximum number of attachments per email	10
Email using	● Microsoft Outlook ○ 3rd Party application
3rd Party application path	
Fax options	
Group by contact information	☑

Name	Copies

There are no items to show.

SYSPRO's archived reports can be retrieved by selecting the *Report Archive* option from the View menu of the SYSPRO Reporting Services program.



Allo...	Activity description	Module	e.net specific activity
☑	PO Req budget deletion	Purchase Orders	
☑	PO Req approve requisition line when price is zero	Purchase Orders	
☑	PO Req approve reqn line when price is zero when approving entir...	Purchase Orders	
☑	PO Cancel partially received lines	Purchase Orders	
☑	PO Complete partially received lines	Purchase Orders	
☑	PO Cancel order with partially received lines	Purchase Orders	
☑	PO Complete order with partially received lines	Purchase Orders	
☑	PO Allow use of any current supplier contract price for Blanket PO	Purchase Orders	
Module: Report Writer			
☑	RW Create reports that update data	Report Writer	
Module: Reporting Services			
☑	SRS Allow maintenance of SRS menu	Reporting Services	
☑	SRS Allow maintenance of SRS forms	Reporting Services	
☑	SRS Allow maintenance of SRS themes	Reporting Services	
☑	SRS Allow purging of SRS archived items	Reporting Services	
☑	SRS View operator group archived items	Reporting Services	
☑	SRS View all archived items	Reporting Services	
☑	SRS Allow report scheduling	Reporting Services	
Module: Return Merchandise Authorization			
☑	RMA Receipt - archive allowed	Return Merchandise Aut...	
☑	RMA Receipt - credit allowed	Return Merchandise Aut...	
☑	RMA Receipt - exchange allowed	Return Merchandise Aut...	
☑	RMA Receipt - fix in-house allowed	Return Merchandise Aut...	
☑	RMA Receipt - inspect allowed	Return Merchandise Aut...	
☑	RMA Allow creation of stocked job	Return Merchandise Aut...	
☑	RMA Cancellation	Return Merchandise Aut...	
	Items:283		

Access rights for retrieving archived reports are defined against your operator using the activities: SRS View operator group archived items and SRS View all archived items.

Summary

Although SYSPRO itself (like all software products) is unable to be certified as Sarbanes-Oxley compliant, this document has highlighted areas where changes can be made to procedures and configuration options to assist your company in becoming compliant. There is also no definitive “If you do this you will be compliant” checklist, so these suggestions should be made in consultation with your Auditors.

Changes to the software are logged on the SYSPRO Support Zone, so this should be viewed regularly. Changes that are significant to Sarbanes-Oxley compliance will be logged under the Sarbanes-Oxley section of the Support Zone.