

Electronic Signatures

SYSPRO 8

Reference Guide

Published: August 2023



CONTENTS

Electronic Signatures

Exploring	1
Starting	4
Solving	5
Using	24

Electronic Signatures

Exploring

Where it fits in?

The **Electronic Signatures** system assists with the effective segregation of duties, as SYSPRO administrators can control who has access to process various transactions. It also enhances governance and traceability by providing an audit trail of who performed a transaction and when it occurred.



This system is commonly used by companies who have requirements for passing corporate governance audits, or who require compliance with various industry regulations such as **FDA 21 CFR Part 11** and the **Sarbanes-Oxley Act**.

Benefits

- Increased transactional security configurable at role, operator, system, company or group level
- Implementation of access control at transaction level rather than only at program level
- Improved governance and traceability of transactions
- Enhanced operations integrity and conformance
- Centralized management for ease of administration
- Elimination of paper document storage as records are displayed on screen, in reports, electronically or PDF format

eSignature Triggers

You can configure **Electronic Signatures** to activate triggers for integration to third-party systems or notification via email (e.g. after adding a customer).

These triggers therefore enable the timely identification of abnormal events or transactions which may potentially indicate fraudulent activity.

You can also define conditional logic so that an eSignature trigger is only fired when additional conditions are met.

Functionality:

- Configure and activate triggers to notify management when significant events occur or to prevent operators from executing various transaction types (e.g. negative receipts).
- Define multiple actions to be executed automatically when an eSignature transaction is successfully completed.
- Invoke **SYSPRO Reporting Services** reports when a trigger is fired.
- Configure VBScripts that can be invoked when a trigger is fired.



This caters for almost unlimited triggering capability, since virtually any type of application can be invoked using VBScript.

Auditing Capabilities

You can configure the **Electronic Signatures** system to maintain a detailed transaction log for auditing purposes (which can be archived for later retrieval).

A computer-generated time-stamp records the date and time of operator entry (including creation, modification, or deletion of records). This lets you generate a secure audit trail of completed transactions, indicating who performed a transaction and when it occurred.

Functionality:

- The **eSignature Query** program provides an audit log of information relating to transactions controlled by eSignatures.
- The **eSignature Report** program lets you generate a report of audit log information relating to transactions requiring eSignatures.
- The **eSignature Purge** program lets you remove audit log entries held on file (based on the age of the entries) to reduce the number of entries in the log table (the table can consume excessive disk space after you have used the **Electronic Signatures** system for some time).

This purge system is controlled using the **Global Configuration** options where you can enable or disable purging and maintain run time selections.

Navigation

The programs related to this feature are accessed from the **Program List** of the SYSPRO menu:

- *Program List > Administration > Electronic Signatures*

Terminology

Electronic Signature

Electronic Signatures (or eSignatures) let you increase control over your system changes by providing security access, transaction logging and event triggering.

This is achieved through the authentication and tracking of system activities against key business processes and sensitive data.

Trigger



This applies to the **Electronic Signatures** system within SYSPRO.

A particular transaction or event initiated or performed by a standard user (i.e. with no administrator permissions) in SYSPRO can fire a particular trigger.

A trigger is the mechanism through which, for example, a VBScript can start running, an email can be sent or another program can be launched.

FOR EXAMPLE:

Changes to supplier details in the **Suppliers** program serve as a trigger for an email notification to a system administrator regarding these changes by a user within your system. This email is sent at the time which changes have been made by a user.

The types of triggers available include:

- Email
- Run a VBScript
- Run any program
- Run any application
- Write to message inbox
- Run an SRS report

Starting

Prerequisites

- You must be a SYSPRO administrator to use the **Electronic Signatures** system.
- The **Electronic Signatures** system must be enabled before using this feature.

Security

You can secure this feature by implementing a range of controls against the affected programs. Although not all these controls are applicable to each feature, they include the following:

- You can restrict operator access to *programs* by assigning them to groups and applying access control against the group (configured using the **Operator Groups** program).
- You can restrict operator access to *programs* by assigning them to roles and applying access control against the role (configured using the **Role Management** program).

Solving

FAQs

Setup and Configuration

How do I enable the Electronic Signatures system?

The system administrator must define the **Global Configuration** settings to enable the **Electronic Signatures** system:

1. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
2. Select the **Global Configuration** function to launch the **Global Configuration** window.
3. Enable the **Electronic signatures required** option.
4. *(Optional)* Disable the **Secure by default** option to ensure that any new eSignature transactions added to the system are automatically defined as **Allowed** by default.



If you leave this option as enabled, then the access control of all new eSignature transactions added to the system are automatically set to **Denied** by default.

5. At the **Authentication by** field, indicate which password must be used for the authentication process when you configure eSignatures that require a password to be entered before certain transactions can be processed.
6. At the **Configuration level** field, indicate the level at which you want to configure eSignatures:
 - **System-wide** (if you want to apply access control and any advanced settings to all operators and groups across the system (i.e. in all companies))
 - **Company, group, operator or role** (if you want to configure eSignatures for a specific company, group, operator or role)
7. *(Optional)* Enable the **Specify company for operator/group/role** option if you want to configure **Electronic Signatures** separately for different companies. Otherwise the configurations defined for each group will apply to those groups in all companies.
8. *(Optional)* Indicate your preferences for purging log records against the **Purge options**.
9. Select the **Save** function to return to the **Electronic Signature Configuration Setup** program.
10. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

How do I add a new configuration level?

The following indicates how a system administrator can create a new eSignature configuration at **Operator, Group, Company** or **Role** level:

1. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
2. Select the **Add a new configuration** toolbar function.
A new blank record is added to the listview.
3. Indicate the **Security level** you require as **Company, Operator, Group** or **Role**.
4. Depending on your selection against the **Security level**, indicate the associated code within the following columns:
 - Company
 - Operator
 - Operator Group
 - Role
5. Indicate the access control you require for this configuration level within the **Transaction type** column:
 - eSignature
 - Allowed
 - Denied
 - Log only
 - Excluded
 - Define by transaction
6. Select the **Save** function.
7. (*Optional*) If you defined the **Transaction type** as `Define by transaction`:
 - a. Select the **Maintain** hyperlink within the **Transactions** column.
This loads the **Electronic Signature Transaction Setup** program from where you can define the transactions associated with the configuration, as well as the trigger and audit log details.
 - b. Locate the transaction you want to configure the eSignature against and select one of the following depending on your requirements:

- To maintain the existing condition for the transaction:
Select the **Edit** hyperlink within the **Edit** column of the **Transactions** listview.
 - To add an additional condition to the transaction:
Select the **Add condition** hyperlink within the **Add condition** column of the **Transactions** listview.
- c. Within **Configure** pane, define the condition as you require it, along with the effective period, logging and trigger requirements.
 - d. Select the **Save** function to return to the **Electronic Signature Configuration Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

How do I create a configuration level at Role level?

You must first define the roles associated with particular operators (within the **Role Management** program) *before* you can add an eSignature configuration at role level (using the **Electronic Signature Configuration Setup** program).

Therefore, you would typically follow this procedure to configure additional settings for your roles system to work with the **Electronic Signatures** system:

1. Open the **Role Management** program (*SYSPRO Ribbon bar > Setup*) to configure your roles for integration with eSignatures.
2. Select the **Global Configuration** option from the **Options** menu:
 - a. Within the **Settings by company within role** section, enable the **eSignatures** option. This lets you assign a company to the operators within a particular role in the **Transactions** listview of the **Electronic Signature Configuration Setup** program.



The **eSignatures always by role** option *doesn't* apply in this context as it only applies to the **Process Electronic Signatures** program which handles the transactional logic of the eSignature system.

- b. Select the **Save and Close** function to return to the **Role Management** program.
3. From the **Role** toolbar field, indicate which role you want to configure for use with eSignatures.
4. Within the **Role Information** pane, select the **Configured by role** option against the **eSignatures** drop-down.
5. Select the **Configure eSignature settings** hyperlink to launch the **Electronic Signature Configuration Setup** program, where a new configuration level is automatically added for the selected role.
 - a. Indicate the access control you require for this configuration level within the **Transaction type** column:
 - eSignature
 - Allowed
 - Denied
 - Log only
 - Excluded
 - Define by transaction
 - b. Select the **Save** function.
 - c. *(Optional)* If you defined the **Transaction type** as `Define by transaction`:

- i. Select the **Maintain** hyperlink within the **Transactions** column.
This loads the **Electronic Signature Transaction Setup** program from where you can define the transactions associated with the configuration, as well as the trigger and audit log details.
 - ii. Locate the transaction you want to configure the eSignature against and select one of the following depending on your requirements:
 - To maintain the existing condition for the transaction:
Select the **Edit** hyperlink within the **Edit** column of the **Transactions** listview.
 - To add an additional condition to the transaction:
Select the **Add condition** hyperlink within the **Add condition** column of the **Transactions** listview.
 - iii. Within **Configure** pane, define the condition as you require it, along with the effective period, logging and trigger requirements.
 - iv. Select the **Save** function to return to the **Electronic Signature Configuration Setup** program.
- d. Exit the **Electronic Signature Configuration Setup** program.
6. Exit the **Role Management** program and restart SYSPRO for your changes to take effect.

How does SSO Identity Provider Integration enhance eSignature security?

When a particular transaction is configured with the highest level of security settings, the operator is required to provide their password each time the transaction is initiated. Moreover, the system allows the administrator to set up an alternative operator password for added flexibility.

During each eSignature password request, the SSO Identity Provider Integration is used for the authentication process. Prior to permitting the transaction to proceed, the system relies on the identity provider to verify the operator's credentials.

This authentication step ensures that only authorized personnel can execute critical transactions, bolstering the overall security and integrity of the eSignature process.

Triggers

How do I send an email for an eSignature transaction or event (i.e. trigger)?

You'd typically follow this procedure to define the details associated with a default email message to be sent when an operator initiates or performs a particular event or activity in your system:

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Define the **Access level** as `eSignature Of Log only`.
4. Within the **Logging and trigger options** section, enable the **Transaction successful** option.
5. Select the **Setup trigger** hyperlink to load the **Trigger Setup** program:
 - a. Select the **New** function from the toolbar to create a new trigger.
 - b. Define the trigger's details as you require:
 - i. Select **Email** against the **Type** drop-down.
 - ii. Indicate a relevant **Description**.
 - iii. Select the **Edit** hyperlink of the **Contents** field to indicate the default email details for a particular trigger (i.e. recipient, subject, contents and any relevant attachments) using the **Send Email** program.
 - iv. Select the **Save** function once you've indicated all the relevant details.
 - c. Exit the **Trigger Setup** program.
6. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.
7. Close the **Electronic Signature Transaction Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

You should now receive a email notification when a SYSPRO operator initiates or performs the particular transaction against which you've defined the conditions.



SMTP emailing is used rather than **Microsoft Outlook** if the eSignature's email trigger is associated with a business object (i.e. the eSignature has *e.net* in the transaction description). Therefore, ensure that your **EMAIL/SMTP SETTINGS** are configured correctly (*Setup Options > System Setup > Connectivity*).

How do I launch a program for an eSignature transaction or event (i.e. trigger)?

You'd typically follow this procedure to load a program once a particular event or transaction has been initiated or performed by a SYSPRO operator.

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Define the **Access level** as `eSignature Or Log only`.
4. Within the **Logging and trigger options** section, enable the **Transaction successful** option.
5. Select the **Setup trigger** hyperlink to load the **Trigger Setup** program:
 - a. Select the **New** function from the toolbar to create a new trigger.
 - b. Define the trigger's details as you require:
 - i. Select **Run any program** against the **Type** drop-down.
 - ii. Indicate the **Program** that you want to run when this trigger is initiated.
 - iii. Select the **Save** function once you've indicated all the relevant details.
 - c. Exit the **Trigger Setup** program.
6. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.
7. Close the **Electronic Signature Transaction Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

The program(s) defined are then automatically launched when a SYSPRO operator initiates or performs the particular transaction against which you've defined the conditions.

How do I send a message to the Message Inbox of another SYSPRO operator for an eSignature transaction or event (i.e. trigger)?

You'd typically follow this procedure to send a message to a single SYSPRO operator, all operators, an entire company, operators within a group or operators within a role once a particular event or transaction has been initiated or performed.

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Define the **Access level** as *eSignature OR Log only*.
4. Within the **Logging and trigger options** section, enable the **Transaction successful** option.
5. Select the **Setup trigger** hyperlink to load the **Trigger Setup** program:
 - a. Select the **New** function from the toolbar to create a new trigger.
 - b. Define the trigger's details as you require:
 - i. Select **Write to message inbox** against the **Type** drop-down.
 - ii. Select the **Edit** hyperlink of the **Contents** field to indicate the details for the default message you want to send to a particular **Security level** group (i.e. a single operator, all operators across a company, etc.) as defined in the **Electronic Signature Configuration Setup** program.
This loads the **Message Inbox Details** window.
 - iii. Indicate the relevant details within the **Message Inbox Details** window.
 - iv. Select the **Save** function once you've indicated all the relevant details.
 - c. Exit the **Trigger Setup** program.
6. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.

7. Close the **Electronic Signature Transaction Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

The applicable operators will then receive a message within their SYSPRO Inbox when a SYSPRO operator initiates or performs the particular transaction against which you've defined the conditions.

How do I launch an application for an eSignature transaction or event (i.e. trigger)?

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Define the **Access level** as `eSignature OR Log only`.
4. Within the **Logging and trigger options** section, enable the **Transaction successful** option.
5. Select the **Setup trigger** hyperlink to load the **Trigger Setup** program:
 - a. Select the **New** function from the toolbar to create a new trigger.
 - b. Define the trigger's details as you require:
 - i. Select **Run any application** against the **Type** drop-down.
 - ii. Indicate the applicable entries within the **Command line** and **Start in** fields.
 - iii. Select the **Save** function once you've indicated all the relevant details.
 - c. Exit the **Trigger Setup** program.
6. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.
7. Close the **Electronic Signature Transaction Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

The application(s) defined are then automatically launched when a SYSPRO operator initiates or performs the particular transaction against which you've defined the conditions.

How do I launch an SRS report for an eSignature transaction or event (i.e. trigger)?

You'd typically follow this procedure to load a SYSPRO Reporting Services report once a particular event or transaction has been initiated or performed by a SYSPRO operator.

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Define the **Access level** as `eSignature Or Log only`.
4. Within the **Logging and trigger options** section, enable the **Transaction successful** option.
5. Select the **Setup trigger** hyperlink to load the **Trigger Setup** program:
 - a. Select the **New** function from the toolbar to create a new trigger.
 - b. Define the trigger's details as you require:
 - i. Select **Run an SRS Report** against the **Type** drop-down.
 - ii. Select the **Edit** hyperlink of the **Contents** field to indicate the applicable report to be used in the condition.
 - iii. Select the **Save** function once you've indicated all the relevant details.
 - c. Exit the **Trigger Setup** program.
6. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.
7. Close the **Electronic Signature Transaction Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

The report(s) defined are then automatically launched when a SYSPRO operator initiates or performs the particular transaction against which you've defined the conditions.

How do I configure user-defined conditions for a specific transaction?

You'd typically follow this procedure to configure additional user defined conditions for a specific transaction in the **Electronic Signatures** system.

FOR EXAMPLE:

You can define a condition against the `WIP Job Creation` transaction to deny an operator from creating jobs for customers who have exceeded their credit limit.

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Select the **User defined** option at the **Condition** field and enter a meaningful description in the **Description** field.
4. Optionally enter a specific condition code within the **Name** field.
5. Select the **Define** hyperlink of the **User condition** field.

Within the **Condition Configuration** pane:

 - a. Add the conditions you require against the transaction.
 - b. Select the **Accept and Close** function.
6. At the **Access level** field, indicate the access control level you require for this new condition. Optionally define an effective period for the condition.
7. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.
8. Close the **Electronic Signature Transaction Setup** program.
9. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

Copying, Importing and Exporting

Why would I want to copy an eSignature configuration?

The copy function is useful for various reasons, some of which include:

- If more than one operator requires the same eSignature configuration, you need only define the configuration for one operator and then use the **Copy From** function to copy that configuration to the other operators.
- If you previously configured eSignatures at operator level but now want to configure at role level, the copy function simplifies the process.

Assuming the eSignature configuration for an operator (or operator group) typifies the configuration you require for the role, you can copy the operator (or operator group) configuration to the new role. Once copied, you can then change the role configuration if required.

This saves you having to entirely re-configure eSignatures for the new role.

Once you have assigned the operator(s) to the roles, you can then delete the individual operator configurations from the **Electronic Signatures** system.

How do I copy eSignature configurations?

You would typically follow this procedure to copy the configuration of **Electronic Signatures** from one operator, company, group or role to another.



This is useful if more than one operator requires the same eSignature configuration as you need only define the configuration for one operator and then use this option to copy that configuration to the other operators.

1. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
2. Highlight the configuration level that you want to copy.
3. Select the **Copy from** function to copy the selected configuration to any configuration displayed in the **Configurations** listview.

This loads the **Copy Selected Configuration to** window.



This is only enabled if your **Security Level** is defined as **Company, Operator, Group** or **Role**.

Or...

Select the **Copy to** function to copy the currently highlighted configuration associated with a particular SYSPRO operator to another operator.

This loads the **Copy configuration: [Operator name] to** window.



This is only enabled if your **Security Level** is defined as **Operator** and the **Specify company for operator/group/role** option within the **Global Configuration** is disabled.

4. Select the **Copy Configuration** function.

The system prompts you to confirm if you want to proceed.

5. Select **Copy Configuration** to confirm the process and copy the configuration.
6. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

How do I export eSignature configurations?

You'd typically follow this procedure to export the eSignature configurations currently displayed in the listview:

1. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
2. Indicate the configurations that you want to export by using the **Select** checkbox (in the **Export** column) against each applicable configuration.



Use the **Select All** toolbar function to export all configurations displayed in the listview.

3. Select the **Export** function.

The **Export Electronic Signatures** window is launched.

4. Indicate the required **File name**.
5. Enable the **Include global configuration** option.



An error is displayed if you don't enable this option, because without this enabled, you won't be able to import the configuration to another system.

6. Select the **Export** function.

An informational message is displayed once this export is successful.

7. Close the **Export Electronic Signatures** window.
8. Exit the **Electronic Signature Configuration Setup** program.

You've successfully exported eSignature configurations and their associated transactions, including the defined triggers and audit log information.

How do I import eSignature configurations?

You'd typically follow this procedure to import eSignatures from a different environment (e.g. a test environment) to your current environment:

1. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).

2. Select the **Import** toolbar function.

The **Import Electronic Signatures** window is launched.

3. Indicate the applicable **File name**.

4. *(Optional)* Enable the **Include global configuration** option so that you don't have to reconfigure the primary settings for the **Electronic Signatures** system after importing the configuration levels.

5. Select the **Import** function.

A warning message is displayed prompting you to proceed with removing all existing configurations. Select **Yes** to continue. Alternatively, select **No** to return to the current window without performing the import.

An informational message is displayed once the import of eSignatures to your current environment is successful.

6. Close the **Import Electronic Signatures** window.

7. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

You've successfully imported eSignature configurations and their associated transactions, including their defined triggers and audit log information.

Auditing

How do I configure a detailed audit log?

You would typically follow this procedure to generate a more detailed log per transaction, apart from the audit log which is generated by default when you set a transaction's access control to **eSignatures** or **Log only**.

In addition, you can add variables to provide insight into transactions performed or initiated by your SYSPRO operators:

1. Load the **Electronic Signature Transaction Setup** program:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Maintain** hyperlink (in the **Transactions** column) against the configuration level for which you want to define conditions. This loads the **Electronic Signature Transaction Setup** program.



This only applies if the **Transaction Type** for the configuration is defined as **Define by Transaction**.

2. Select the **Edit** hyperlink against the relevant transaction within the **Transactions** listview. Alternatively, select the **Add condition** hyperlink to add an additional condition. This enables the **Configure** pane.
3. Define the **Access level** as `eSignature Or Log only`.
4. Enable the **Detail log required** option under the **Logging and trigger options** section.
5. Optionally select the **Configure details** hyperlink to load the **Configure Detail Log** window:
 - a. Indicate the variables that you want to include in the detailed log for the transaction by using the checkbox within the **Select** column.

FOR EXAMPLE:

You may want to know the name of the supplier and banking details associated with the supplier that was added by an operator for the `AP Supplier added` transaction.

You'd therefore add the `%Key`, `%Bank`, `%BankAccount` and `%BankBranch` variables.



Adding a large number of variables to the detail log can increase the size of the audit log table. Therefore, you should consider only including the required variables.

- b. Select **Ok** to save your selections.

6. Select the **Save** function of the **Electronic Signature Transaction Setup** program to save your condition's configuration.
7. Close the **Electronic Signature Transaction Setup** program.
8. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.

You can now view the audit logs for eSignature transactions using the **eSignature Query** program (*Program List > Administration > Electronic Signatures*).

How do I generate a report of audit logs for eSignatures?

The **eSignature Report** program lets you generate a report of audit log information relating to transactions requiring eSignatures:

1. Open the **eSignature Report** program (*Program List > Administration > Electronic Signatures*).
2. Indicate if you want to generate a **Detail** or **Summary** report at the **Report type** field.
3. (*Optional*) Indicate your criteria preferences for which you want to generate the report.
 - Transaction selection
 - Transaction date selection
 - Transaction time selection
 - Operator selection
 - Program selection
 - Key selection
 - Variable selection
4. (*Optional*) Use the **Include** options to define which transaction statuses you want to include in the report.
5. (*Optional*) Define any additional report options you require within the **Output Options** pane.
6. Select the **Process** function.
7. Exit the **eSignature Report** program.



Using this lets you produce a report of the audit entries displayed in the **eSignature Query** program according specific report criteria and report options.

How do I view detailed information regarding audit logs?

To view the audit log of eSignature transactions processed, proceed as follows:

1. Open the **eSignature Query** program (*Program List > Administration > Electronic Signatures*).
2. Indicate the relevant **Time filter**.
3. Enable the **Show detail** option from the toolbar.
4. Optionally define any criteria you require within the Filter Options pane and select the **Apply Custom Filter** function.
5. Select the **Refresh View** function.

How do I purge audit logs for eSignatures?

After defining your preferences for purging log records, you can use the **eSignature Purge** program to remove audit log entries held on file, based on the age of the entries:

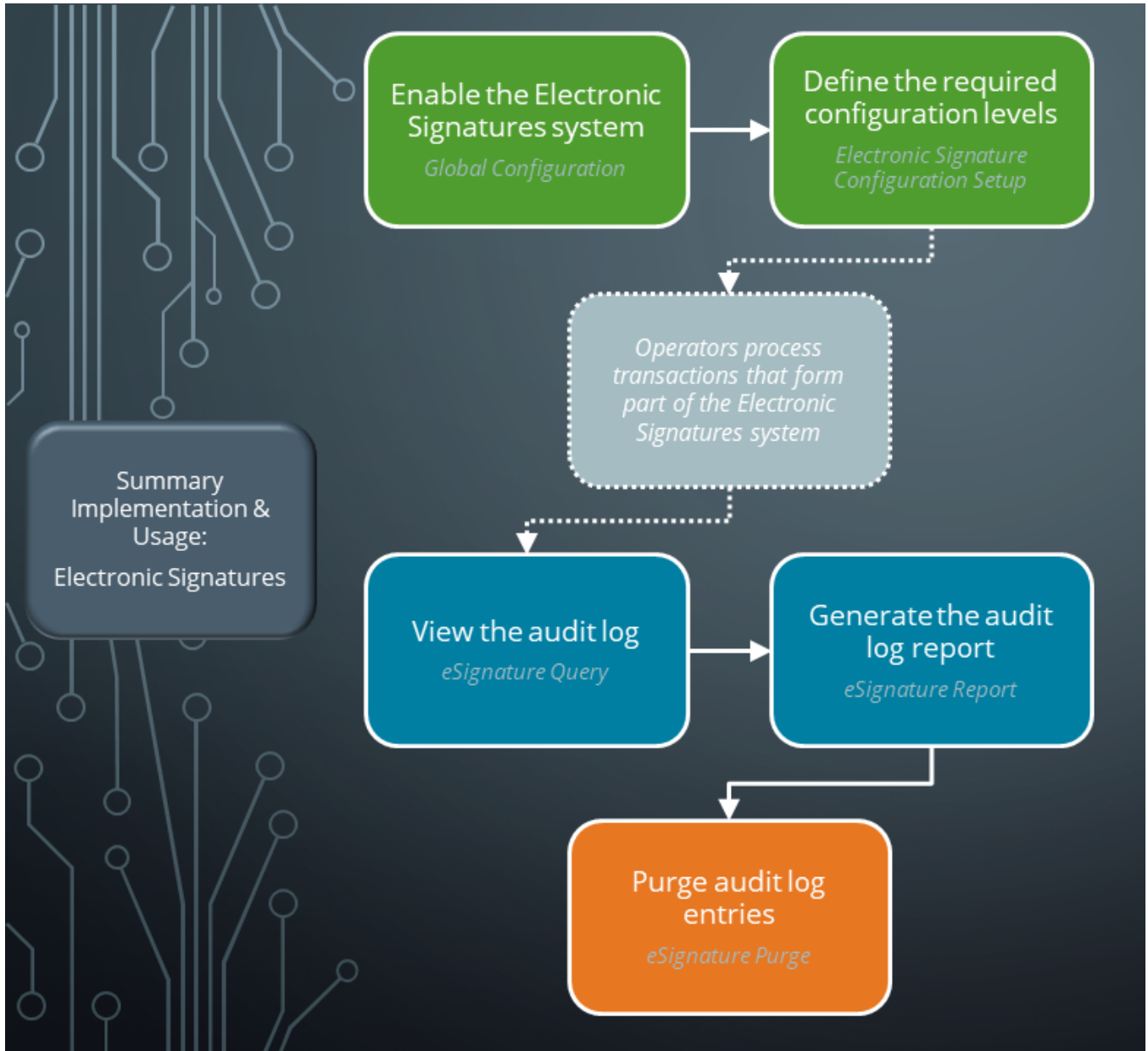
1. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - a. Select the **Global Configuration** function to load the **Global Configuration** window.
 - b. From the **Purge options** section, select the **Allow purge** option to enable purging audit logs for eSignatures.
 - c. Optionally enable the **Allow run time selection** option so that you can indicate the relevant number of months or years against the **Purge log records older than** drop-down.
 - d. Select the **Save** function.
You are returned to the **Electronic Signature Configuration Setup** program.
 - e. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.
2. Open the **eSignature Purge** program (*Program List > Administration > Electronic Signatures*).
 - a. At the **Purge** field, indicate if you want to remove all audit log information or only the details log.
 - b. Use the slider to indicate the **Months to retain records**.
 - c. Select the **Start purge** function and accept the confirmation message that is displayed.

The program automatically closes and an informational message is displayed indicating how many records were removed.

Using

Process

Summary implementation and usage



The following process outlines how to implement the **Electronic Signatures** system for a single company. However, this is only a basic guide and you can configure the system differently according to your requirements:

1. Enable the **Electronic Signatures** system:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Global Configuration** function to launch the **Global Configuration** window.
 - c. Enable the **Electronic signatures required** option.
 - d. (*Optional*) Disable the **Secure by default** option to ensure that any new eSignature transactions added to the system are automatically defined as **Allowed** by default.



If you leave this option as enabled, then the access control of all new eSignature transactions added to the system are automatically set to **Denied** by default.

- e. At the **Authentication by** field, indicate which password must be used for the authentication process when you configure eSignatures that require a password to be entered before certain transactions can be processed.
 - f. At the **Configuration level** field, indicate the level at which you want to configure eSignatures:
 - **System-wide** (if you want to apply access control and any advanced settings to all operators and groups across the system (i.e. in all companies))
 - **Company, group, operator or role** (if you want to configure eSignatures for a specific company, group, operator or role)
 - g. (*Optional*) Enable the **Specify company for operator/group/role** option if you want to configure **Electronic Signatures** separately for different companies. Otherwise the configurations defined for each group will apply to those groups in all companies.
 - h. (*Optional*) Indicate your preferences for purging log records against the **Purge options**.
 - i. Select the **Save** function to return to the **Electronic Signature Configuration Setup** program.
 - j. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.
2. Define your configuration level(s) at **Operator, Group, Company** or **Role** level:
 - a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - b. Select the **Add a new configuration** toolbar function.
A new blank record is added to the listview.

- c. Indicate the **Security level** you require as **Company, Operator, Group** or **Role**.
- d. Depending on your selection against the **Security level**, indicate the associated code within the following columns:
 - Company
 - Operator
 - Operator Group
 - Role
- e. Indicate the access control you require for this configuration level within the **Transaction type** column:
 - eSignature
 - Allowed
 - Denied
 - Log only
 - Excluded
 - Define by transaction
- f. Select the **Save** function.
- g. *(Optional)* If you defined the **Transaction type** as `Define by transaction`:
 - i. Select the **Maintain** hyperlink within the **Transactions** column.

This loads the **Electronic Signature Transaction Setup** program from where you can define the transactions associated with the configuration, as well as the trigger and audit log details.
 - ii. Locate the transaction you want to configure the eSignature against and select one of the following depending on your requirements:
 - To maintain the existing condition for the transaction:

Select the **Edit** hyperlink within the **Edit** column of the **Transactions** listview.
 - To add an additional condition to the transaction:

Select the **Add condition** hyperlink within the **Add condition** column of the **Transactions** listview.
 - iii. Within **Configure** pane, define the condition as you require it, along with the effective period, logging and trigger requirements.
 - iv. Select the **Save** function to return to the **Electronic Signature Configuration Setup** program.

- h. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.
3. Once the **Electronic Signatures** system is in place and operators have begun processing transactions that form part of your configuration level(s), you can view the audit log:
 - a. Open the **eSignature Query** program (*Program List > Administration > Electronic Signatures*).
 - b. Indicate the relevant **Time filter**.
 - c. Enable the **Show detail** option from the toolbar.
 - d. Optionally define any criteria you require within the Filter Options pane and select the **Apply Custom Filter** function.
 - e. Select the **Refresh View** function.
4. Generate a report of audit log information relating to transactions that form part of the **Electronic Signatures** system:
 - a. Open the **eSignature Report** program (*Program List > Administration > Electronic Signatures*).
 - b. Indicate if you want to generate a **Detail** or **Summary** report at the **Report type** field.
 - c. (*Optional*) Indicate your criteria preferences for which you want to generate the report.
 - Transaction selection
 - Transaction date selection
 - Transaction time selection
 - Operator selection
 - Program selection
 - Key selection
 - Variable selection
 - d. (*Optional*) Use the **Include** options to define which transaction statuses you want to include in the report.
 - e. (*Optional*) Define any additional report options you require within the **Output Options** pane.
 - f. Select the **Process** function.
 - g. Exit the **eSignature Report** program.
5. If required, you can purge the audit log entries held on file to reduce the size of the log files:

- a. Open the **Electronic Signature Configuration Setup** program (*Program List > Administration > Electronic Signatures*).
 - i. Select the **Global Configuration** function to load the **Global Configuration** window.
 - ii. From the **Purge options** section, select the **Allow purge** option to enable purging audit logs for eSignatures.
 - iii. Optionally enable the **Allow run time selection** option so that you can indicate the relevant number of months or years against the **Purge log records older than** drop-down.
 - iv. Select the **Save** function.

You are returned to the **Electronic Signature Configuration Setup** program.
 - v. Exit the **Electronic Signature Configuration Setup** program and restart SYSPRO for your changes to take effect.
- b. Open the **eSignature Purge** program (*Program List > Administration > Electronic Signatures*).
 - i. At the **Purge** field, indicate if you want to remove all audit log information or only the details log.
 - ii. Use the slider to indicate the **Months to retain records**.
 - iii. Select the **Start purge** function and accept the confirmation message that is displayed.

The program automatically closes and an informational message is displayed indicating how many records were removed.

Access Control Levels

Within the **Electronic Signatures** system, you can define access control either at configuration or transaction level. Therefore, the following table summarizes the access control levels available.

Considerations:

- The access levels you define against an individual operator take precedence over the access levels defined at company level.
- Each transaction condition can have a different access control level.

Similarly, each operator group can be assigned a different access level.



- If you select the **eSignature** or **All Secured by eSignature** access level, then a password must be defined against each operator who has access to the transaction. This is either an operator password or an alternate password, depending on your selection at the **Authentication by** option within the **Global Configurations**.
- Where transactions are configured against a specific operator, the access level defined against the operator applies (except if this access level is set to **Excluded from definition**), regardless of the configuration against any groups to which the operator belongs.

If the access method for a transaction configured against an operator is defined as **Excluded from definition**, then the access level defined against the operator's group (s) applies.

If the access level against the group(s) is also set to **Excluded from definition**, then the access level defined against the company applies.

Access Control	Impact
<p>eSignature (Configuration level) or eSignature (Transaction level)</p>	<p>This sets the current transaction or configuration level to be subject to the Electronic Signatures system.</p> <p><i>Configuration level</i></p> <p>Transactions are subject to Electronic Signatures and therefore operators must enter a password before a transaction can be processed.</p> <p><i>Transaction level</i></p> <p>The transaction is subject to Electronic Signatures and you therefore need to indicate one of the following against the transaction:</p> <ul style="list-style-type: none"> ▪ The operator is required to confirm with a password to proceed. ▪ A message box should be displayed requesting confirmation, with a default result to either proceed or deny the transaction. <p><i>Auditing capabilities</i></p> <p>An audit log is generated for each transaction when this access control is defined at either level.</p>
<p>Allowed (Configuration level) or Allowed (Transaction level)</p>	<p>When selected at either Configuration or Transaction level: Operators can process transactions without having to enter a password (i.e. transactions are ignored by the Electronic Signatures system).</p> <p><i>Auditing capabilities</i></p> <p>No audit log is generated for the transaction.</p>
<p>Denied (Configuration level) or Denied (Transaction level)</p>	<p>When selected at either Configuration or Transaction level: Operators are prevented from processing any SYSPRO transaction that forms part of the Electronic Signatures system.</p> <p><i>Auditing capabilities</i></p> <p>No audit log is generated for the transaction.</p>

Access Control	Impact
<p>Log Only (Configuration level)</p> <p>or</p> <p>Log only (Transaction level)</p>	<p>When selected at either Configuration or Transaction level:</p> <p>Operators can process transactions, but an audit log is generated for every transaction. In other words, this is the same access control as Allowed, except an audit log is generated.</p> <p><i>Auditing capabilities</i></p> <p>An audit log is generated for each transaction when this access control is defined at either level.</p>

Access Control	Impact
<p>Excluded (Configuration level)</p> <p>or</p> <p>Excluded from definition (Transaction level)</p>	<p>When selected at either Configuration or Transaction level: Transactions are ignored by the Electronic Signatures system.</p> <div data-bbox="520 405 1378 595" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> You would typically select this option at Configuration level if you wanted to configure only a few transactions for Electronic Signatures.</p> </div> <p><i>Configuration level considerations</i></p> <p>The access control to all transactions are set to <code>Excluded</code>. You can then select the Define by Transaction option to configure the transactions you want to secure individually.</p> <p>If you select this option but do not configure any transactions individually, then this is equivalent to selecting the Allowed option for the selected configuration level.</p> <p>Therefore, the purpose of this option at Configuration level is to cascade the access level up to the next level defined, except when using role-based eSignature definitions, as there are no higher-up levels.</p> <div data-bbox="520 1137 1378 1397" style="border-left: 2px solid #333; padding-left: 10px; margin: 10px 0;"> <p>FOR EXAMPLE:</p> <p>If the transaction is excluded for an operator, then the access level defined against the group applies.</p> <p>If this is defined as <code>Excluded from definition</code>, then the access level defined against the company applies.</p> </div> <div data-bbox="520 1420 1378 1570" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> This access control is an advanced option and should therefore only be used with sophisticated conditional logic.</p> </div> <p><i>Auditing capabilities</i></p> <p>No audit log is generated for the transaction.</p>

Access Control	Impact
Define by Transaction (Configuration level)	<p>When selected at Configuration level:</p> <p>This lets you configure each SYSPRO transaction that forms part of the Electronic Signatures system individually.</p> <p>You can then select the Edit or Add condition option from the Transactions listview of the Electronic Signature Transaction Setup program to define additional configuration options for each transaction.</p> <p>In addition, you can deselect individual transactions in the Transactions listview, thereby setting that transaction to Denied for the selected configuration level.</p>

Transaction Security Level Hierarchy

Transactions can be configured with different security levels for all operators, by operator or by group. In addition, each transaction can be configured with multiple conditions.



You can configure up to 50 user-defined conditions for a single transaction.

Therefore, it is crucial to understand the security level hierarchy in both single and multiple Operator/Group/Company configurations:

Single Operator/Group/Company Configuration

If a transaction is configured for a single operator/group/company, with multiple conditions, and all of these conditions are true, then the following hierarchy is used to determine which condition applies:

Denied takes precedence, followed by:

1. eSignature
2. Log only
3. Allowed
4. Excluded from definition

Therefore, if the condition is true and the security level is set to **Denied**, then this will override any other conditions for the transaction.

The following illustrates the hierarchy used for processing multiple conditions in a single Operator/Group/Company configuration:

- If "condition 1" is defined as **Denied**:
Then the security level for the transaction is set to **Denied**, regardless of what access control is set for "condition 2".
- If "condition 1" is defined as **eSignature**:
Then the security level for the transaction is set to **eSignature**.
Exception: If the access control for "condition 2" is defined as **Denied**, then "condition 2" takes precedence.
- If "condition 1" is defined as **Log only**:
Then the security level for the transaction is set to **Log only**.
Exception: If the access control for "condition 2" is defined as **Denied** or **eSignature**, then those access levels take precedence.
- If "condition 1" is defined as **Allowed**:
Then the security level for the transaction is set to that of "condition 2".

- *Exception:* If the access control for "condition 2" is defined as **Excluded from definition**, then "condition 1" takes precedence.
- If "condition 1" is defined as **Excluded from definition**:
Then the security level for the transaction is set to that of "condition 2".

FOR EXAMPLE:

The following indicates an example of the hierarchy used for access control in a single Operator/Group/Company configuration:

You use the **Add condition** option to define the following against a transaction:

Name	Access control level	Condition
Condition 1	Log only	Whenever stock on hand changed.
Condition 2	Allowed	Stock on hand < Safety level.
Condition 3	Denied	Stock on < 0.

If all the above conditions are true, then the security level **Denied** applies.

If the first and second conditions were true, then **Log only** applies.

Multiple Group Configurations

For each group, for the current transaction, it must be determined which security level applies. If there are multiple conditions, then this security level is determined as described above.

Where an operator belongs to multiple groups, the following security hierarchy is used to determine which group's configuration applies:

eSignature takes precedence followed by:

1. Log only
2. Allowed
3. Access denied
4. Excluded from definition

Therefore, if the operator belongs to any group where **eSignature** is configured for the current transaction, then this overrides any other conditions configured for another group for the same transaction.

The following illustrates the hierarchy used for processing multiple groups:

- If "group 1" is defined as **Denied**:

Then the security level for the transaction is set to that of "group 2".

Exception: If "group 2" has the access level defined as **Excluded from definition**, then "group 1" takes precedence.

- If "group 1" is defined as **eSignature**:

Then the security level for the transaction is set to **eSignature**, regardless of what access control is defined against "group 2".

- If "group 1" is defined as **Log only**:

Then the security level for the transaction is set to **Log only**.

Exception: If "group 2" has the access level defined as **eSignature**, then "group 2" takes precedence.

- If "group 1" is defined as **Allowed**:

Then the security level for the transaction is set to **Allowed**.

Exception: If "group 2" has the access level defined as **eSignature** or **Log only**, then "group 2" takes precedence.

- If "group 1" is defined as **Excluded from definition**:

Then the security level for the transaction is set to that of "group 2".

Status Codes

Electronic Signatures - Transaction Statuses

The following indicates the different statuses which may apply at some point to each transaction that forms part of the **Electronic Signatures** system.



You can view the current status of an eSignature transaction using the **eSignature Query** program or the **eSignature Report**.

Status	Description
<p>0 - AUTHORIZED BUT NOT YET COMPLETE</p> <p>Successfully passed Electronic Signature verification (but transaction not yet completed)</p>	<p>This status indicates that the transaction has been authorized but not yet completed.</p> <p>FOR EXAMPLE:</p> <p>If the AP Month-end performed transaction is configured within the Electronic Signatures system to require a password before proceeding, and an operator enters the correct password but has not yet completed the full process, then the transaction resides in this status until complete.</p>
<p>1 - FUNCTION CANCELED</p> <p>Operator canceled from Electronic Signature function</p>	<p>This status indicates that the operator canceled the particular function before the eSignature verification could complete.</p> <p>FOR EXAMPLE:</p> <p>The Access Control against the against the AP Delete payment run transaction was defined as Allowed, but the operator canceled the process while performing a payment run.</p>
<p>2 - PASSWORD VERIFICATION FAILED</p> <p>Failed to enter password x number of times</p>	<p>This status indicates that the password verification failed due to the operator entering the incorrect password x number of times.</p>
<p>3 - DENIED ACCESS</p> <p>Operator was denied access to the function</p>	<p>This status indicates that the operator was denied access to the particular function or transaction.</p> <p>FOR EXAMPLE:</p> <p>The operator couldn't perform the month-end as the Access control defined against the CB Month-end performed transaction was defined as Denied.</p>

Status	Description
<p>4 - TRANSACTION CANCELED</p> <p>Operator canceled the transaction</p>	<p>This status indicates that the operator canceled the transaction before it completed.</p>
<p>9 - AUTHORIZED AND COMPLETE</p> <p>Transaction was authorized completed successfully</p>	<p>This status indicates that the transaction has been successfully authorized and completed.</p> <p>FOR EXAMPLE:</p> <p>If the Access control against the AP Post invoice transaction for a particular operator is defined as Allowed and that operator then processes an invoice, the transaction is successfully authorized and completed.</p>

Affected programs

The following indicates areas in the product that may be affected by implementing this feature:

Setup programs

Electronic Signature Configuration Setup

Program List > Administration > Electronic Signatures

This program lets you enable the **Electronic Signatures** system and create or maintain your eSignature configuration levels and their associated access control.

Electronic Signature Transaction Setup

*(Accessible via the **Maintain** hyperlink of the **Transactions** column within the **Electronic Signature Configuration Setup** program)*

This program lets you configure specific transaction conditions against your eSignature configuration levels.

Trigger Setup

*(Accessible via the **Setup trigger** hyperlink of the **Logging and Trigger** options within the **Electronic Signature Transaction Setup** program)*

This program lets you assign multiple actions that can be executed automatically when an eSignature transaction is successfully completed.

The actions that can be triggered include the following:

- Email
- Run a VBScript
- Run any program
- Run any application
- Write to message inbox
- Run an SRS report

Generic Condition Maintenance

*(Accessible via the **Define** hyperlink of the **User condition** field within the **Electronic Signature Transaction Setup** program)*

This program lets you add conditional statements for user-defined conditions against eSignature transactions.

Period End programs

eSignature Purge

Program List > Administration > Electronic Signatures

This program lets you remove audit log entries relating to transactions that form part of the **Electronic Signatures** system, based on the age of the entries.

Report programs

eSignature Report

Program List > Administration > Electronic Signatures

This program lets you generate a report of audit log information relating to transactions that form part of the **Electronic Signatures** system.

Query programs

eSignature Query

Program List > Administration > Electronic Signatures

This program lets you view an audit log of information relating to transactions controlled by the **Electronic Signatures** system.



www.syspro.com

Copyright © SYSPRO. All rights reserved.
All brand and product names are trademarks or
registered trademarks of their respective holders.

