



ENOVIA SmarTeam

SmarTeam – Regulatory Compliance Framework User Guide

© Dassault Systèmes, 2006, 2009. All rights reserved.

CATIA, ENOVIA, SMARTEAM and the 3DS logo are registered trademarks of Dassault Systèmes or its subsidiaries in the US and/or other countries.

PROPRIETARY RIGHTS NOTICE: This documentation is the property of Dassault Systèmes. This documentation shall be treated as confidential information and may only be used by employees or contractors of the Customer in accordance with the terms of the End-User License Agreement accepted by Customer.

Any use of the Licensed Program contained in this media or accompanying it, is subject to the terms of the End User License Agreement accepted by Customer. The Licensed Program is protected by international copyright laws and international treaties. Unauthorized use, reproduction and/or distribution of any of the Licensed Program, or any part thereof, may result in severe civil and/or criminal penalties, and will be prosecuted to the maximum extent possible under the law. Company names and product names mentioned herein are the property of their respective owners and certain portions of the Licensed Program contain elements subject to copyright owned by these entities. See the Documentation CD provided with the Licensed Program for details and/or additional terms and conditions relating to these entities.

Part Number: RCF-U1-190409

Contents

Contents	i
Chapter 1: Overview	1
Introduction	1
Software Location	1
Related Documentation	1
Internet Site	2
.....	2
Chapter 2: Getting Started	3
What is an Electronic Signature?	3
How Electronic Signature Can Help You	3
People Involved in the Electronic Signature Procedure	4
Meaning of Signature	4
Audit Trail	4
Chapter 3: Defining Electronic Signatures in the Flowchart Designer	5
How to Define Electronic Signatures	5
Chapter 4: Configuring the Electronic Signature	11
Chapter 5: Signing the Documents	14
Chapter 6: Setting Up the Audit Trail	16
Setting Up the Audit Trail for the Login Process	17
Monitoring Lifecycle Operations with Audit Trail	18
Enabling the Viewing of Audit Trail Records	18
Chapter 7: Viewing Audit Trails	20
Enhanced Security	21

Chapter 1: Overview

Introduction

SmarTeam – Regulatory Compliance Framework provides a working environment and functionality, which accelerates the process by which organizations ensure compliance to industrial regulations, such as the FDA (Food and Drug Administration).

SmarTeam – Regulatory Compliance Framework ensures and facilitates the following:

- High-level authentication security
- Management of electronic records
- Electronic signatures within approval processes
- Execution of automated tasks

One of the requirements of the Regulatory Compliance Framework is the Job Server, which automates tasks carried out by a server. For more information, see the SmarTeam – Job Server Online Help.

All user functionality and procedures for using the SmarTeam – Regulatory Compliance Framework functionality are described in this guide.

Installation and setup procedures for SmarTeam – Regulatory Compliance Framework software are described in the SmarTeam – Regulatory Compliance Framework Installation and Setup Guide.

For additional information about SmarTeam functionality, see the SmarTeam – Editor User Guide.

Software Location

The information described in this guide is for the SmarTeam – Regulatory Compliance Framework (Electronic Signature) software, which is available through the SmarTeam – Editor.

Related Documentation

The following documents are referred to in this guide. All of these documents are available on the ENOVIA SmarTeam Documentation CD.

Document	Remarks
SmarTeam – Regulatory Compliance Framework Installation and Setup Guide	This document explains the procedures required to install SmarTeam – Regulatory Compliance Framework.
SmarTeam – Job Server Online Help	Describes how to use the Job Server.
SmarTeam – Editor Administrator Guide	Provides administration procedures to customize and maintain SmarTeam – Editor.
SmarTeam – Editor Installation Guide	This document explains the procedures required to install the SmarTeam – Editor.
SmarTeam – Web Editor Installation Guide	This document explains the procedures required to install the SmarTeam – Web Editor.

Internet Site

You are highly recommended to frequently visit our website for the latest updates and plug-in products, including the latest Service Packs, Program Directory (Release Notes), Hotfixes and technical support at <http://support.smarteam.com/>.

Chapter 2: Getting Started

What is an Electronic Signature?

An electronic signature is a digitally encrypted signature on a document or any class in SmarTeam. For example, to approve a 2D CAD sketch of a bolt, the designer's manager and the QA department must sign the sketch.

Within SmarTeam, an electronic signature can be tied to any SmarTeam object (of different leaf/super-classes).

IMPORTANT! An electronic signature can only be activated through a Workflow process.

An electronic signature is assigned to an object through a Workflow process, which must include the following two nodes:

- The first node activates the Electronic Signature Configuration tool, which defines the number of signatures and the number of users who can sign per predefined Electronic Signature node.
- At least one node where the users who should sign the document are assigned.

See SmarTeam – Workflow Online Help for details about setting up the Workflow.

Note: The SmarTeam – Regulatory Compliance Framework is installed while installing the SmarTeam – Editor, which includes all the necessary components for both the SmarTeam – Editor SmarTeam – Web Editor.

How Electronic Signature Can Help You

Part 11 regulations require that certain Electronic Records requiring a signature have a mechanism in place to manage the signatures. If the signature is managed electronically, the Electronic Signature must be uniquely identified by the Electronic Record. This Electronic Signature guarantees signer authenticity, data integrity, and non-repudiation of electronic documents. Electronic Signatures can be implemented independently.

People Involved in the Electronic Signature Procedure

There are three types of people involved in the Electronic Signature procedure:

- An administrator who sets up the Electronic Signature flowchart, and defines which nodes in the flowchart require electronic signatures. The administrator sets up the electronic signature by defining the parameters, script hooks and policies in the Electronic Signature Workflow nodes. The administrator could be, for example, someone from the company's IT department.
- A technical manager who specifies which documents/objects need signatures, and at which nodes the signatory can view the document information and approve it.
- The signatory, who signs and approves the documents, according to the rules defined by the technical manager. The signatory signs the documents by selecting values for each parameter shown. After signing, the signatory validates the signature. The signatory could be, for example, a Team Leader, a QA person, or a Documentation person.

Meaning of Signature

Each company can define the Meaning of Signature attribute as free text or as a lookup table for each Electronic Signature node. The Meaning of Signature attribute can be defined at the process level or at the node level.

To define the Meaning of Signature attribute:

- 1 In the Admin Setting class in the database, find/create the section named `MeaningOfSignatureDefinition`.
- 2 Assign the section a subject name, such as `<Flowchart Name_Node Description>`, where:
 - `Flowchart Name` is the name of the flowchart for which the Meaning of Signature is defined.
 - `Node Description` is the name of the node for which the Meaning of Signature is defined (optional). If a Node Description is not specified the definition is applied to all the nodes in the flowchart.

Note: One section should be created for each flowchart name and node description.

- 3 Specify values for the Meaning of Signature in the `Long Value` field.
 - a For lookup tables, the values should be delimited by semicolons as shown below:


```
<value1>;<value2>;<value3>
```

 For example, `Approve;Confirm;Reject`
 - b For free text, leave this field blank.

See [Chapter 5, “Signing the Documents”](#) for an example of how the Meaning of Signature appears in the Electronic Signature.

Audit Trail

The purpose of the Audit Trail is to monitor different activities in the database.

The Audit Trail can be run in both SmarTeam – Web Editor and SmarTeam – Editor.

Chapter 3: Defining Electronic Signatures in the Flowchart Designer

Because the electronic signature is part of the SmarTeam – Regulatory Compliance Framework, it is associated with any SmarTeam object (e.g. different super/leaf classes).

The administrator configures the electronic signatures in the Flowchart Designer.

The administrator determines which nodes in the flowchart have electronic signatures and who can sign them. The administrator then configures each of these nodes specifically for the electronic signature.

This section is intended for use by the administrator.

Notes:

- Objects of different super-classes cannot be attached to the same flow process for Electronic Signatures. For example, to define Electronic Signatures for Items and Documents, two flow processes must be used.
- Throughout this Guide, the term “document” is used. However, an electronic signature may be assigned to any object that belongs to a class for which the Electronic Signature mechanism has been defined in the Data Model Designer (DMD), such as Items, CAD drawings, CATIA Parts.

For more information on the Flowchart Designer, see the SmarTeam – WorkFlow Online Help.

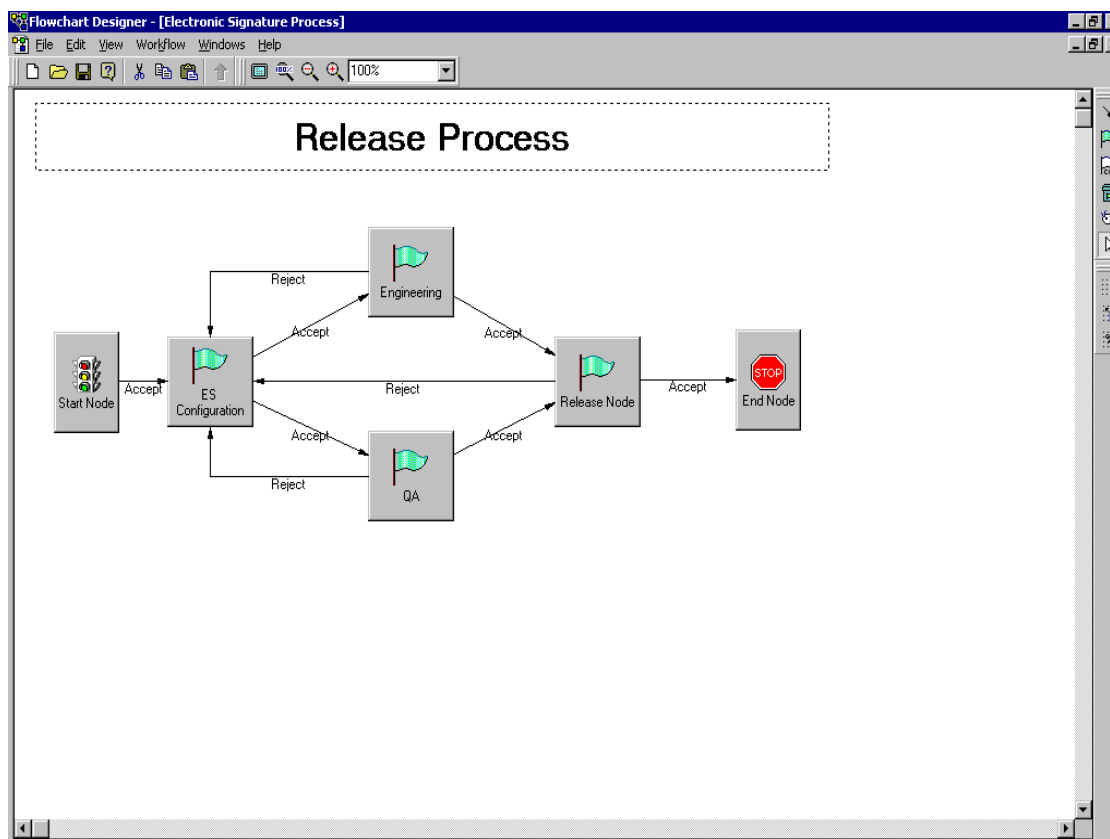
How to Define Electronic Signatures

To define electronic signatures:

- 1 Open the Flowchart Designer with the appropriate flowchart.

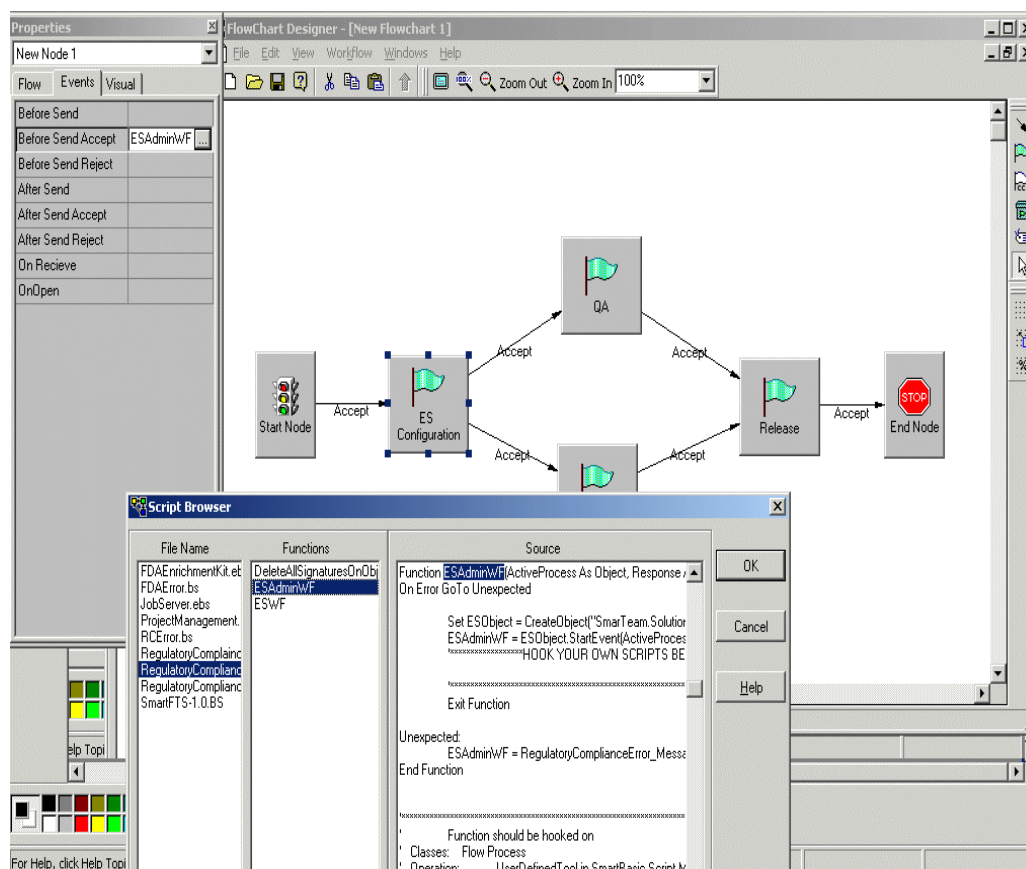
2 Select the **ES Configuration** node.

This node is responsible for presenting the table (names of nodes that have signatures) for the signatory to sign.



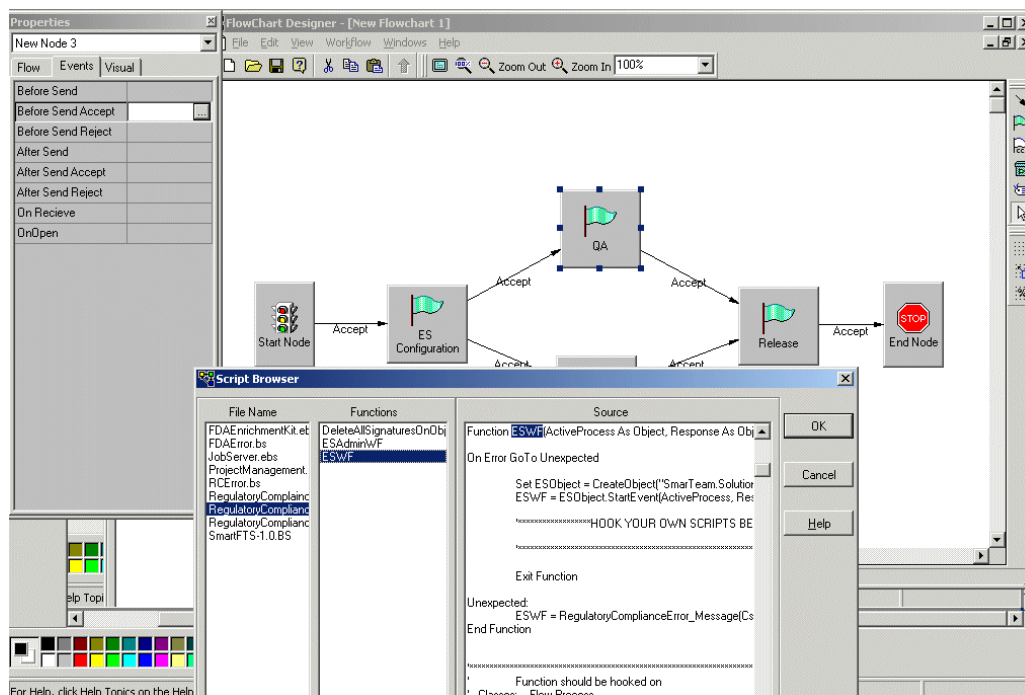
3 Double-click the **ES Configuration** node to open the Properties window.


4 In the **Before Send Accept** event, hook the **ESAdminWF** function from the **RegulatoryCompliance.ebs** file.



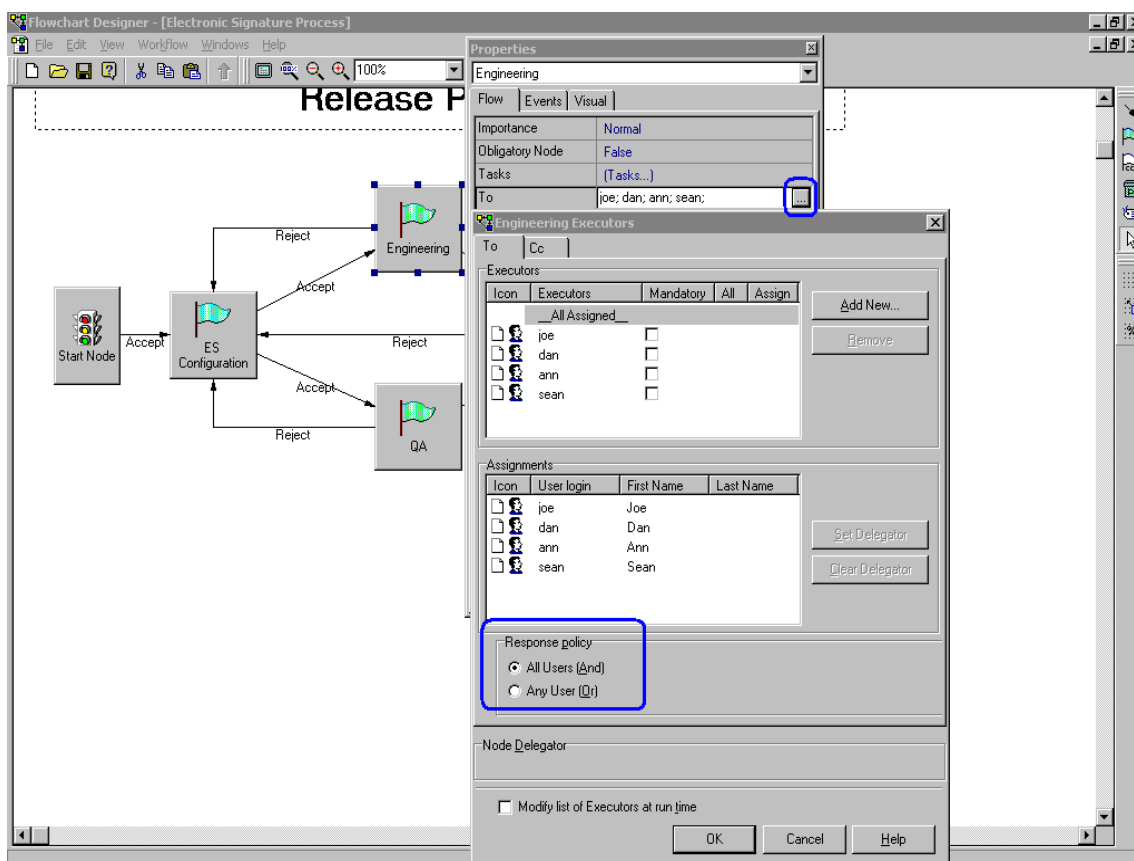
- 5 In the table presented to the signatory, only those nodes assigned as having electronic signatures appear. To implement this, you must configure each of these nodes as follows.
 - a Double-click on a desired node to open the Properties window.
 - b In the **Before Send Accept** event, hook the **ESWF** function from the **RegulatoryCompliance.ebs** file.

Note: If you want to use a customized script, create an administration setting with Section: **ES_UPGRADE** and Subject: **SIGN_SCRIPT_NAME**. Complete the Section field with the name of your script and send the script as an attachment instead of ESWF.



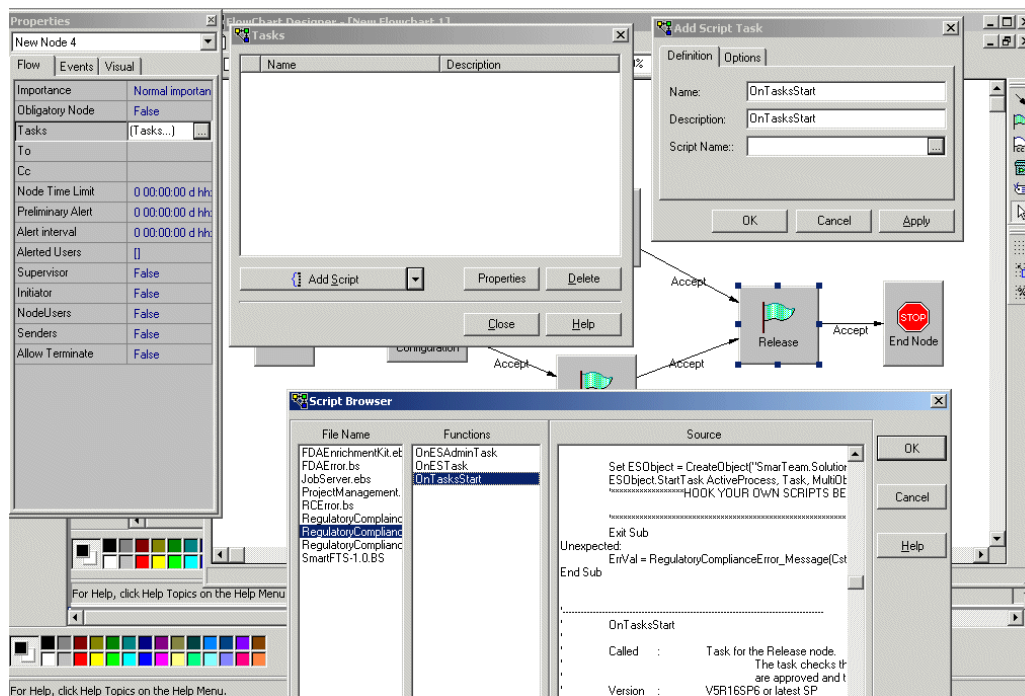
- 6 For each node that includes an electronic signature, you can also define a Response Policy by doing the following.
 - a Double-click on the node.
 - b From the Properties window, select the Flow tab, and click the Browse button  in the To field.

The Engineering Executors window appears.



- 7 In the Response Policy area, select a response policy according to the requirements for this Electronic Signature. This setting determines what the manager sees when setting up the Electronic Signature for the signatories:
 - All Users (And) includes two values: All/None
 - Any User (Or) includes two values: One/None
- 8 Double-click on the Release node to set up the release of the documents after all the documents have been signed.

9 Select the **OnTaskStart** task script from the **RegulatoryCompliance.ebs** file.



This script performs the release operations, and creates a job that maps fields for signature to the documents. The job is handled by the Job Server. For additional details about the Job Server, see the *SmarTeam – Job Server Administration Guide*.

Chapter 4: Configuring the Electronic Signature

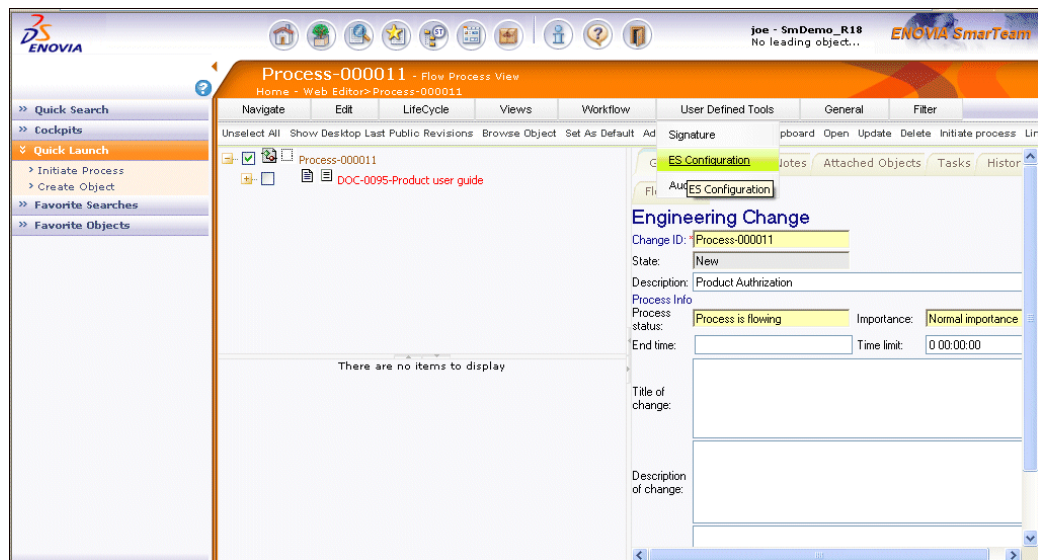
To configure the Electronic Signature, the manager selects the documents to be signed and the people who can sign them.

Configuring the Electronic Signature is performed by a person who understands the documents to be signed and who knows who the signatories should be, such as the manager of a department or a team leader.

This section is intended for the administrator responsible for configuring the Electronic Signature.

To configure the Electronic Signature:

- 1 From Actions menu, select **ES Configuration**.

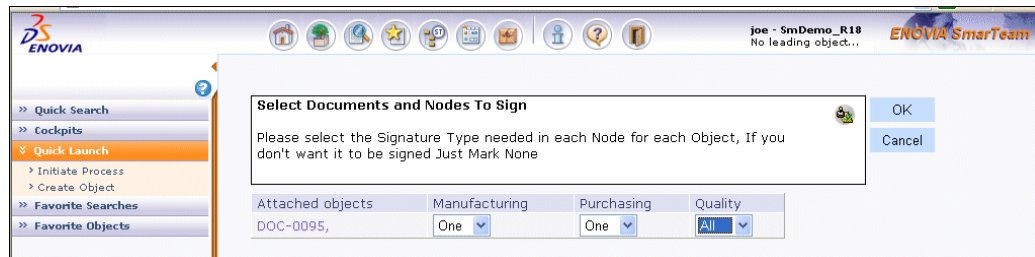


The documents presented in the resulting User Defined Tools window are attached to the process that are currently in Check-In mode. Documents attached to the process that have Electronic Signatures defined in another flow process do not appear in this window.

- 2 From the User Defined Tools window, select who should sign the document (as defined by the Administrator in the Response Policy) for each document as follows.

- **One** - Only one signatory needs to sign this document.
- **All** - All signatories need to sign this document.
- **None** - No signatories need to sign this document. If this option is selected, the document will not appear in the list of documents seen by the signatory.

Note: Before selecting, you can view the Profile Cards of the documents listed in this window by clicking on their links.



Only the nodes with an Electronic Signature appear. For each node, one column is presented. QA and Engineering nodes have Electronic Signatures. For more information, see [Step a](#) in the section about how to define nodes for Electronic Signatures.

- 3 After selecting the settings, select **Accept** from the Actions menu to complete this stage.

IMPORTANT! You cannot select **Accept** before configuring the Electronic Signatures. If you select **Accept** before completing the configuration process, the system automatically displays the first Configuration window.

Adding an Electronic Signature to a Profile Card

As part of the Electronic Signature mechanism, two attributes are available, which an administrator can add to the profile card of objects signed with electronic signatures.

- **ES Details:** Contains the following Attributes: Process ID+ Node Name+ User Name (the one that signed) + meaning of Signature + Date time for each node that is signed.

Example:

Process: Process-000022

Node Name: Formulation User name:: Joe Davis Meaning Of Signature:
Approved by ZSV Date:: 2/12/2009 2:25:35 PM

Node Name: New Node 5 User name:: Joe Davis Meaning Of Signature:
second signature Date:: 2/12/2009 2:35:26 PM

- **ES Status:** Object Status in the process (Pending, Complete or Not needed)

Removing an Electronic Signature and its Details

In the RegulatoryCompliance.ebs script file there are several functions that delete all the signatures and its details, such as ES status and ES details, from an object/process:

- DeleteAllUserSignaturesOnObject – Deletes signatures from an object
- DeleteAllUserSignaturesOnObjectEx – Deletes signatures from object extensions

- DeleteAllUserSignaturesOnProcess – Deletes signatures from a process
- DeleteAllUserSignaturesOnProcessEx – Deletes signatures from process extensions

These functions can be hooked to operations such as, Check Out, Update, NewRelease, which are appropriate to customer business practice.

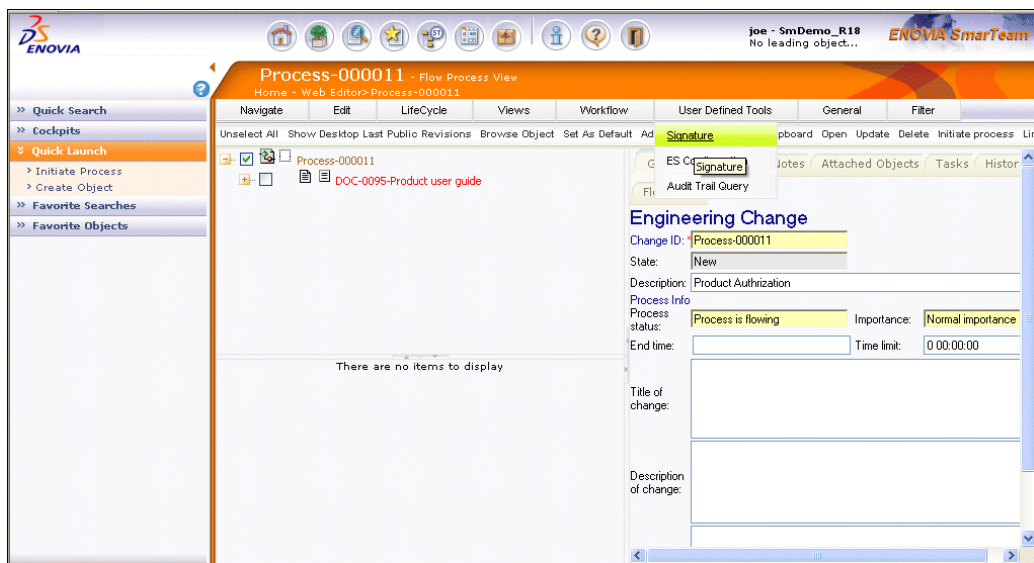
Chapter 5: Signing the Documents

This section is intended for use by the signatory of the documents.

Note: To sign a document in SmarTeam, the document must be in Check-In mode.

To sign the documents:

- 1 From the Actions menu, select **Signature**.



- 2 From the Electronic Signature window, select the **Sign** check box for each document you want to sign.

Notes:

- The Date and Time presented are GMT.
- The User Name, Date and Current Node fields are disabled, and cannot be changed.
- Before signing documents, you can view the Profile Cards of the documents listed in this window by clicking on their links.

The screenshot shows the ENOVIA User Defined Tools interface. The left sidebar contains a navigation menu with options: Quick Search, Cockpits, Quick Launch (selected), Initiate Process, Create Object, Favorite Searches, and Favorite Objects. The main area displays the 'Electronic Signature' dialog box. It contains a message: 'Please select the objects that the Electronic Signature applies to, select a signature meaning and verify your approval by signing your SmarTeam User Name and Password'. Below this are input fields for 'User name:' (Joe Davis), 'Date:' (04/26/2007 13:04), and 'Current node:' (Purchasing). There are 'OK' and 'Cancel' buttons. At the bottom, there is a table with three columns: 'Sign', 'Attached objects', and 'Meaning Of Signature'.

Sign	Attached objects	Meaning Of Signature
<input checked="" type="checkbox"/>	DOC-0095,	

- 3 Select an option from the Meaning of Signature list, or type in the meaning of the signature in this field, and click **OK**.

Note: The Meaning of Signature field may be defined as free text (default) or as lookup values in the AdminSettings class. It can be configured with one type for each node or for each flow chart. If it is defined as lookup values, the user sees the values in a drop-down list.

- 4 From the Electronic Signature Validation dialog box type your User name and Password and click **OK**.

The Electronic Signature Validation dialog box appears for security purposes to ensure that no unauthorized person signs a document.

The screenshot shows a 'Signin -- Web Page Dialog' window titled 'Electronic Signature validation'. It contains input fields for 'User name' (joe) and 'Password' (masked with dots). There are 'OK' and 'Cancel' buttons. The status bar at the bottom shows the URL 'http://172.16.105.129/WebEditor/' and the 'Internet' icon.

- 5 From the Actions menu, select **Accept** to accept the Electronic Signature process.

IMPORTANT! You cannot select **Accept** before signing the documents. If you select **Accept** before completing the signature process, the system automatically displays the first Signature window, which is useful if the user does not realize the document must be signed.

Chapter 6: Setting Up the Audit Trail

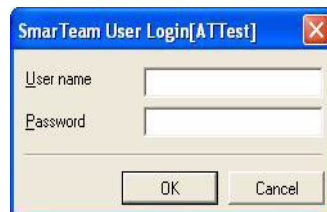
The purpose of the Audit Trail is to monitor different activities in the database. The Audit Trail can be run in both SmarTeam – Web Editor and SmarTeam – Editor.

The following steps must be performed to set up and run the Audit Trail:

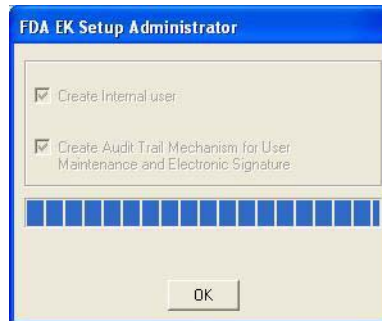
- 1** From **<SmarTeamDirectory>\Bin** run the SmarTeam.Solutions.RegulatoryComplianceSetupAdministrator tool to set the Audit Trail to work on User Maintenance activities (groups, roles, users, and relationships between them, permissions) in both SmarTeam – Editor and SmarTeam – Web Editor, by doing the following:
 - a** Select the database on which this tool should run.



- b** Type the administrator User name and Password to log in to SmarTeam and click **OK**.



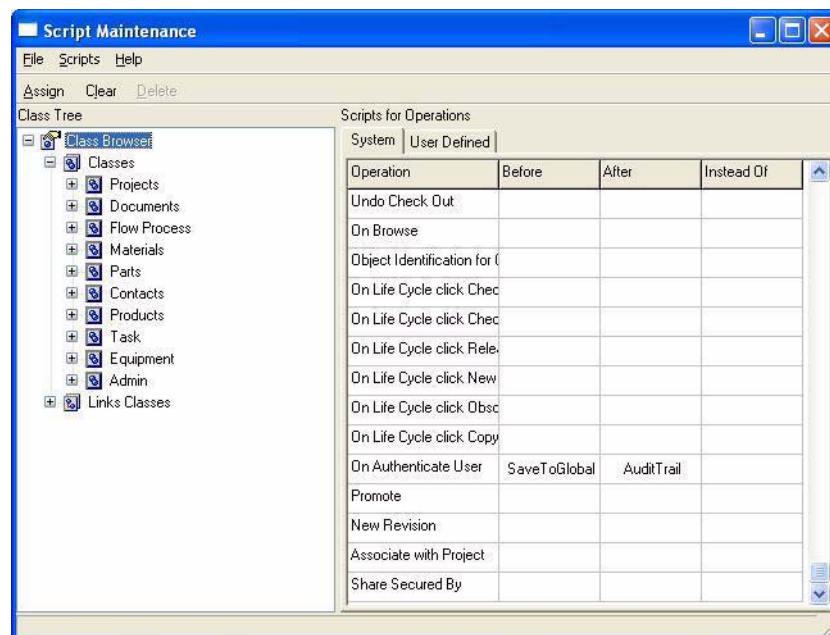
- c** Let the tool run and add the scripts to SmarTeam. Then, exit the tool by clicking **OK**.



Setting Up the Audit Trail for the Login Process

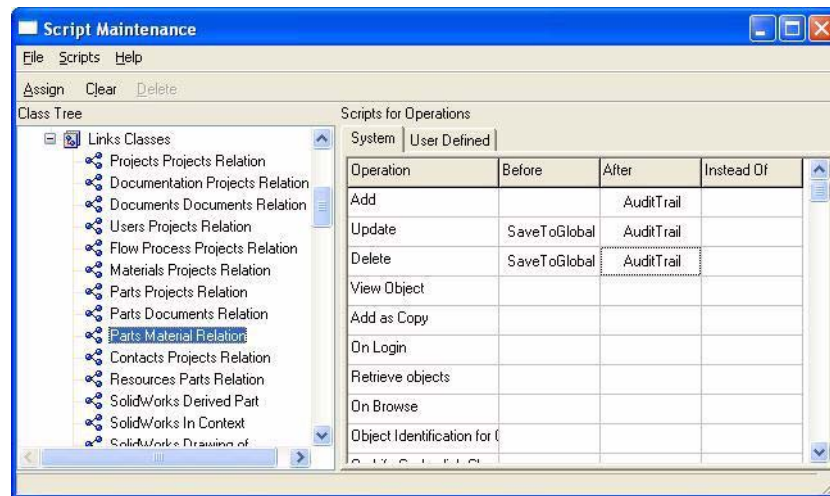
For the Login process (Success, User Locked, etc.), run the Audit Trail as follows:

- 1 Attach a hook to a script in Script Maintenance in the **OnUserAuthentication** event in the Before and After stages. The scripts to be added can be found in the **RegulatoryCompliance.ebs** file. To attach the hook set the following:
 - Before: **SaveToGlobal**
 - After: **AuditTrail**



- 2 Select the different classes on which the Audit Trail should be performed, such as documents, and connect the scripts as described in [Step 1](#).
 - a If you want to monitor adding documents, in Script Maintenance, in the **Add** event, set the following:
 - Before: **SaveToGlobal**
 - After: **AuditTrail**

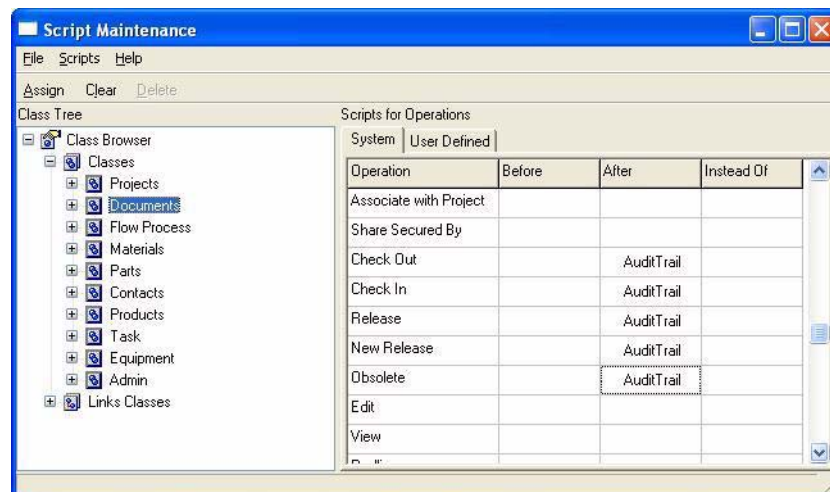
- b Repeat this process for link classes, hierarchical links and link relations (one-level links).



Monitoring Lifecycle Operations with Audit Trail

To monitor Lifecycle operations (for Revision-Managed classes only):

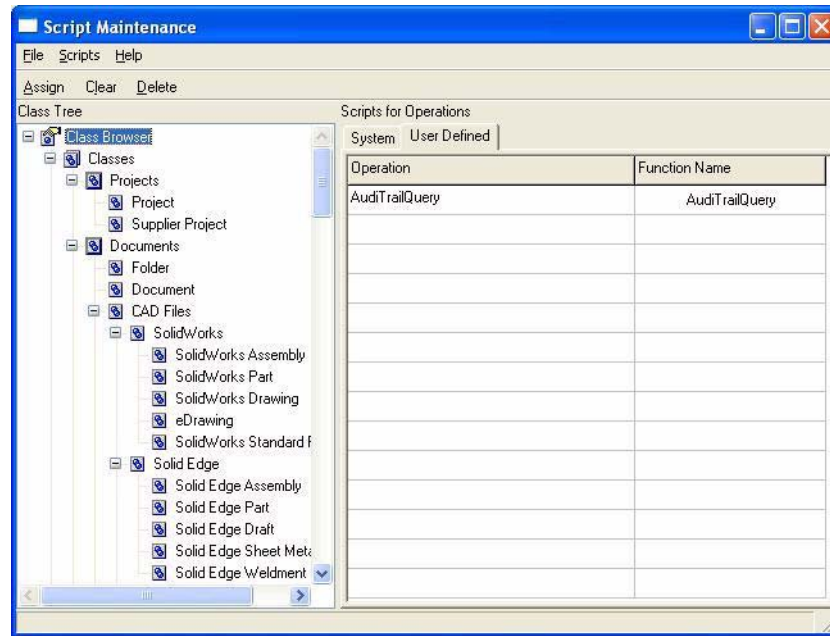
- Attach **AuditTrail** to **After<lifecycle-operation>**, such as **AfterCheckIn**, **AfterCheckOut**, **AfterRelease**, **AfterNewRelease**, **AfterObsolete**.



Enabling the Viewing of Audit Trail Records

To enable the viewing of Audit Trail records in SmarTeam – Editor:

- 1 Add a user-defined event with any name, such as **Audit Trail Query**, and attach it to the script **AuditTrailQuery** in the **RegulatoryCompliance.ebs** file.



- 2** To enable this tool in the SmarTeam – Web Editor, add a **UserDefinedTool** key. This key should be added to **SmarTeam\Configuration Settings\Data\Domain\smarteam.std.webEditor.config.xml**.

Notes:

- If the xml file **smarteam.std.webEditor.config.xml** does not exist under **Domain** it should be available under **Default**. Copy it to the **Domain** level where you should type this configuration key value.

For example, for the **Audit Trail Query** tool, add the following code under the **UserDefined-Tools** key:

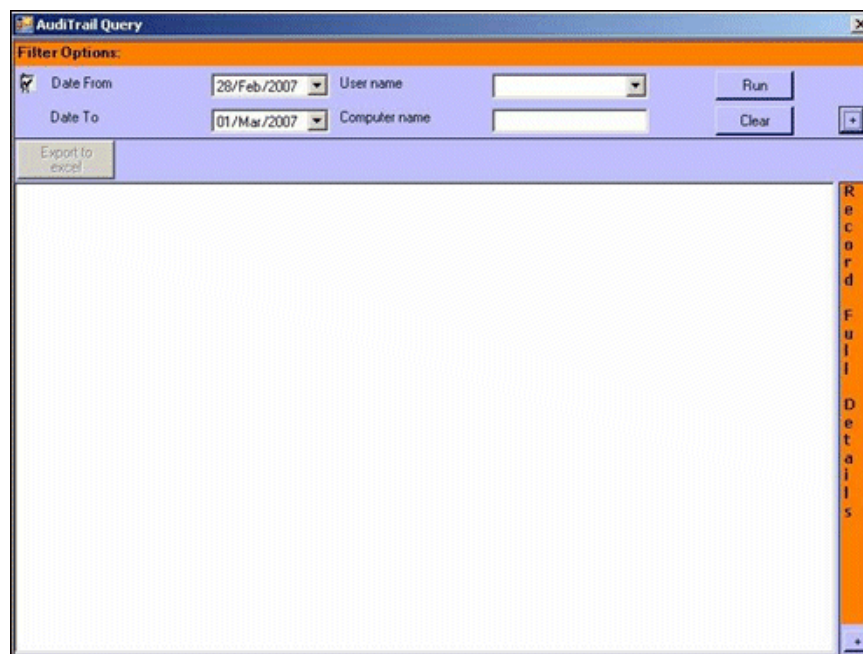
```
<userDefinedTool>
  <operationName>AuditTrailQuery</operationName>
  <pageName>SmarTeam.Solutions.AudiTrail.GUI.Web/AuditTrailQuery.aspx
  </pageName>
</userDefinedTool>
```

- The Operation name (operationName) in the xml must be the same as the name in [Step 1](#).
- To perform an audit on the SmarTeam – Web Editor, you must configure the xml accordingly. Details about the configuration are available in the “Server Hooks Configuration” section in Chapter 5 of the SmarTeam – Regulatory Compliance Framework Installation and Setup Guide.pdf.

Chapter 7: Viewing Audit Trails

The Audit Trail can be viewed by running the appropriate user-defined tool on the item as defined in [Enabling the Viewing of Audit Trail Records](#).

When the Audit Trail is run, the following window appears:



From the Filter Options area (top of window), you can define the filter options for the Audit Trail records you want to see.

For advanced filter options, click the + button on the right side of the window in the Filter Options area.

You can also export the data to Excel.

Note: To enable exporting of AuditTrail records in the SmarTeam – Web Editor to Excel, you must enable/prompt all ActiveX activation through scripts. This is accomplished by accessing the **Security > Custom Security** Internet option and enabling all ActiveX initialization procedures.

After the Audit Trail is run, the Audit Trail data is presented as follows:

AuditTrail Query

Filter Options:

☒ Date From: 01/Mar/2007 User name:

Date To: 27/Mar/2007 Computer name:

ID	Date	User name	NT User Name	Computer name	Operation	Alert	Audited ID	Description
2007Mar0612	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0612	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0612	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0612	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0602	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0602	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0612	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0612	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0602	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0603	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0604	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0605	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0605	06/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0702	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0703	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0704	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0704	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0705	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0705	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use
2007Mar0705	07/Mar/2007	HSysManage	Administrator	NirV17	Login	Normal	HSysManage	'Login'. Use

Record Full Details

Enhanced Security

When an administrator creates a new user, the following actions occur:

- The user is assigned an **Inactive** state.
- A temporary random password is automatically created and sent from the system via Mail Job. The password is created according to the following rules:
 - The password matches the configuration defined by the User Account management tool.
 - The algorithm used for the password is MD5 (encrypted). It is mandatory for the administrator to set MD5 password algorithm when using RCF.
 - The Password expiration date is the date on which the password is created. To define the password expiration, navigate to Administrator options in SmarTeam – Editor. Select User Account Preferences options > Password. Define the required settings.

In addition:

- When an administrator releases a locked user (after too many incorrect logins), a new password is automatically sent to the user.
- When an administrator changes the password algorithm from plain text to MD5, the user automatically receives a new password.

Notes:

- To enable enhanced security, configure the SmarTeam – Job Server and configure the Mail Executable for the SmarTeam – Job Server.
- For additional information about setting up the SmarTeam – Job Server, see the SmarTeam – Job Server Online Help.