



## **ENOVIA SmarTeam**

# **SmarTeam – Regulatory Compliance Framework Administration Guide**

---

© Dassault Systèmes, 2006, 2010. 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-U1-200410

# Contents

<b>Chapter 1: Overview</b>	<b>1</b>
Introduction	1
Related Documentation	2
Internet Site	2
<b>Chapter 2: Installation</b>	<b>3</b>
Hardware and Software Requirements	3
Order of Installation	3
<b>Chapter 3: RCF Setup</b>	<b>4</b>
Adding Mechanisms to Database	4
Server Hooks Configuration	6
Define and Update Profile Cards	6
SmarTeam User Profile Card	7
Profile Cards for Classes with Electronic Signature Mechanisms	7
Profile Cards of Admin Classes	7
Importing LDAP Users	7
<b>Chapter 4: Electronic Signature</b>	<b>8</b>
Methodology	8
Electronic Signatures Process Definition	8
Electronic Signatures Stages	8
Electronic Signature Attributes	9
Meaning of Signature	9
Configurations	9
Electronic Signatures Stages Implementation	9
Configuring the Electronic Signature Workflow	10
ES Configuration Node	11
Signature Nodes	11
Node for Release	12
Define Meaning of Signature Attributes	13
Other Scripts of Electronic Signature	14
How to use an Electronic Signature	14
<b>Chapter 5: Audit Trail</b>	<b>17</b>
Methodology	17
Configuration	17

Audit Trail Script .....	17
Audit Trail Supported Hooks and Classes .....	18
Audit Trail Hooks for Internal Classes .....	18
Merging Scripts .....	19
Enabling the Viewing of Audit Trail Records .....	19
How to use Audit Trail .....	19
<b>Chapter 6: Enhanced User Security .....</b>	<b>22</b>
Configuration .....	22
Admin Settings .....	22
General Settings .....	23
Harden User Security .....	23
Minimum Password Length .....	23
New User Creation .....	24
<b>Appendix A: Define RCF User Defined Tools for Work in SmarTeam – Web Editor</b> .....	<b>25</b>
<b>Appendix B: RCF Internal Classes .....</b>	<b>26</b>
Electronic Signature .....	26
Audit Trail .....	26
<b>Appendix C: RCF Upgrade Mechanism .....</b>	<b>27</b>
Upgrade Process .....	27
Database Preparations .....	28

# Chapter 1: Overview

## Introduction

SmarTeam – Regulatory Compliance Framework (RCF) 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:

- Electronic Signature Management

- What is an Electronic Signature?

An electronic signature is a digital signature on a document or any SmarTeam objects that is managed by the customer. For example, to approve a 2D CAD sketch of a bolt managed in a SmarTeam document, the designer's manager and the QA department should sign the sketch.

- How Can Electronic Signature Help You?

Part 11 regulations define that certain electronic records requiring a signature have a mechanism in place to manage signatures. If a 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.

- Supervision of SmarTeam User Activities

The Audit Trail is used to supervise SmarTeam users for the following activities: Add, Update, Delete, Lifecycle operations and Login of the user to the system. These activities are saved in the database and can be viewed by the administrator via a dedicated tool.

- Enhanced User Authentication Security

To complete the regulatory compliance requirements, an administrator can define restricted security for user management and control users who can access the system using advanced options.

For example, a user password should be:

- Encrypted using the MD5 algorithm
- Set to expire after a predefined number of days
- Locked if a user fails to log in several times

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 Administration Guide.

This guide provides all the information necessary for a SmarTeam system administrator regarding RCF installation, functionality and procedures for using RCF functionality.

The RCF is supported by SmarTeam – Editor and SmarTeam Web 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 – Job Server Administration Guide	Provides the necessary information for a SmarTeam system administrator to setup 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://www.3ds.com/support/>.

In addition, you can also view any installation known issues.

## Chapter 2: Installation

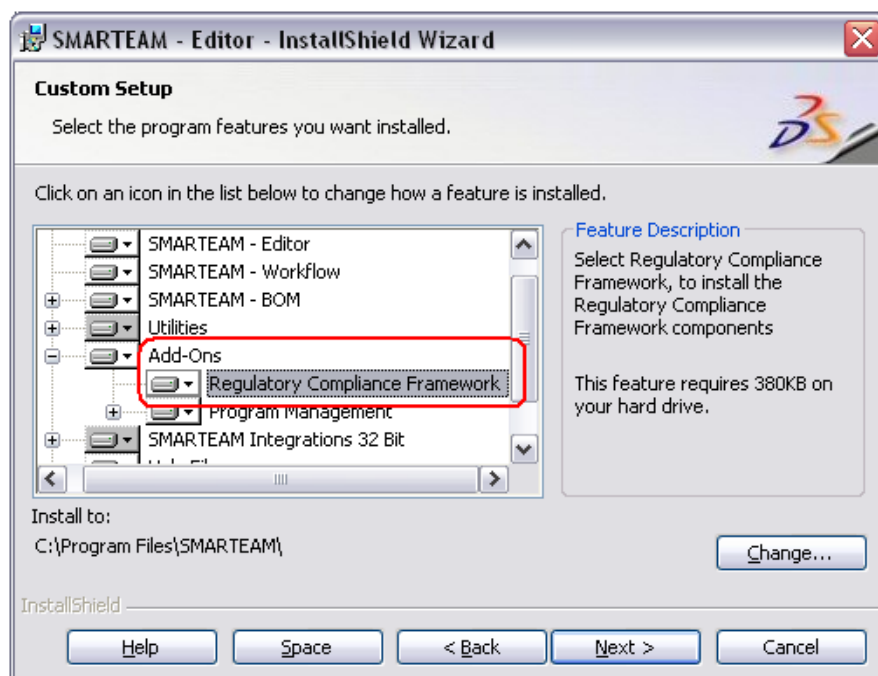
### Hardware and Software Requirements

There are no specific Hardware and Software Requirements for RCF software.

### Order of Installation

SmarTeam – Foundation with the Workflow components must be installed on your computer before you install the RCF.

RCF is installed while installing the SmarTeam – Editor. The location of RCF is under the Add-Ons (see following image).



**Note:** If RCF is used in the database, then this installation, which includes all the necessary components, should be installed for all SmarTeam – Editor clients including the SmarTeam – Web Editor server.

## Chapter 3: RCF Setup

After software installation of the RCF, you must perform all the stages in this chapter before you can use the RCF product.

### Adding Mechanisms to Database

To work with the Electronic Signature you must add the relevant mechanisms to your database using the SmarTeam Data Model Designer utility. This operation, which only adds the relevant mechanisms, does not affect the SmarTeam Data Model structure.

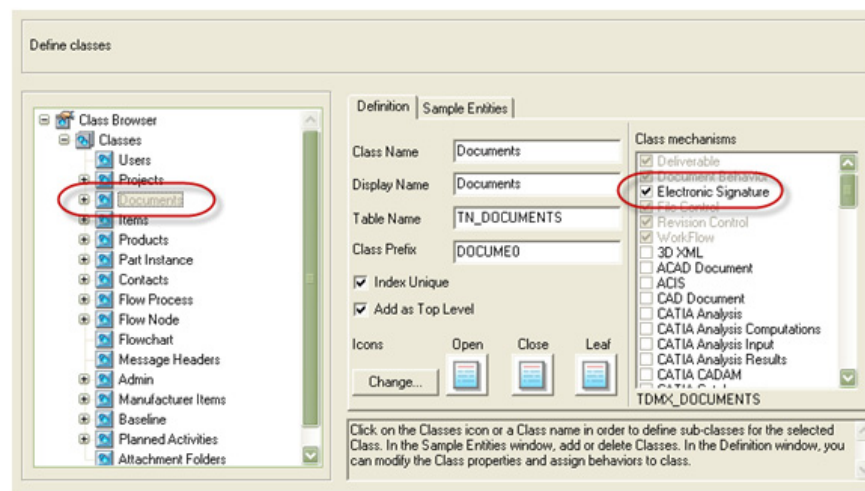
**Note:** It is highly recommended that you perform a backup operation of the selected database before performing this update procedure.

#### *To update your selected database:*

- 1** From the taskbar Start button, select **Programs > SmarTeam > Administrative Tools > SmarTeam Data Model Designer** to launch the SmarTeam Data Model Designer.
- 2** In the Data Model Designer window, select **File > Modify Database Structure** from the main menu to display the Available Databases window.
- 3** In the Available Databases window, select the required database and click **OK**.  
A SmarTeam message window appears, advising you to perform a backup of the selected database before proceeding to update the selected database.
- 4** Verify you back up your database and click **Yes**.
- 5** The Wizard Login [Database Name] window appears. Type the applicable Username and Password for the selected database and then click **OK** to continue.  
After a successful login, the SmarTeam Data Model Designer window displays the selected database.
- 6** The following new mechanisms are available in the SmarTeam Data Model Designer utility:
  - Electronic Signature
  - Audit Trail
  - Job Server (must be selected)
  - Admin (may already be selected in the database)
- 7** Select mechanisms and click **Next**.



- 8 In the Define Classes window, activate Electronic Signature mechanism on Classes required signature:
  - Select a Class to which you want to add the Electronic Signature mechanism (such as Documents).
  - The mechanism can be added to a Super Class, Sub-class or Leaf -class, as required.
  - In the Class mechanisms pane, select Electronic Signature.
  - Repeat this step for each Class requiring the Electronic Signature mechanism.
- 9 Example: In this illustration Documents has been selected as the class to which the Electronic Signature mechanism has been activated.



- 10 Click **Create** to update the database structure according to your selections in the previous steps.

The Changes in Class Tables window appears showing pertinent information for updated classes.

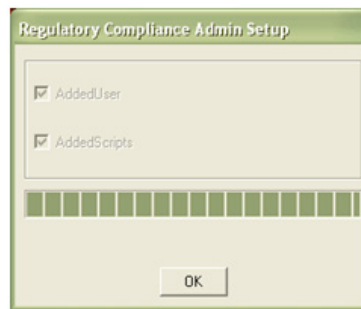
Classes are updated according to your Electronic Signature requirements.

- 11 In the Changes in Class Tables window, click **OK** to start the update process. This process may take a long time depending on the size of the selected database and the number of changes performed.
- 12 When you receive a system message that the database has been successfully modified, click **OK** to save changes and exit the SmarTeam Data Model Designer.

#### To run RCF Admin Setup:

- 1 From <SmarTeamDirectory>\Bin run:  
SmarTeam.Solutions.RegulatoryComplianceSetupAdministrator.Exe
- 2 Select the database on which this tool should run.
- 3 Type the administrator Username and Password to log in to SmarTeam and click **OK**.
- 4 Let the tool run. Then, exit the tool by clicking **OK**.

**Note:** This tool adds internal user and attach scripts for internal classes for the Audit Trail of the Login to SmarTeam and Enhanced User Authentication Security.



## Server Hooks Configuration

To ensure RCF is fully operational over the Web, SmarTeam administrator should add several definitions to System Configurations. Use the System Configuration Editor to add them if you can. If System Configuration Editor cannot be used, you can make changes to the System Configuration by manually updating the XML files in the System Configuration.

**Note:** In all the XML files the value of the System Configuration Key must be after the configuration code.

Verify that the relevant value exists for each of the following keys and if not, update it accordingly. These keys must be defined according to the following list so the RCF works properly.

- ServerHooks.CLSID

```
<ServerHooks.CLSID>{82F7EBD2-61D9-4CEB-8FD8-535EF32DEB2C}</ServerHooks.CLSID>
```

- ServerHooks.Init

```
<ServerHooks.Init>SmarTeam.Solutions.RegulatoryComplianceSH.csRCFunctions.cs</ServerHooks.Init>
```

**Notes:** Notes:

- The keys should be defined in Domain or System level.
- The files are defined in: smarteam.std.legacypreferences.config.xml.

## Define and Update Profile Cards

Using the Form Designer and Web Form Designer utility, update the following Profile Cards:

- SmarTeam User Profile Card
- Profile Cards for classes to which the Electronic Signature mechanisms is added
- Profile Cards of Admin Classes

## SmarTeam User Profile Card

The SmarTeam User Profile Card > Info tab page, must contain the following properties: User Login, First Name, Last Name and Email.

## Profile Cards for Classes with Electronic Signature Mechanisms

The following are Profile Cards for classes to which Electronic Signature mechanisms are added. Class Profile Cards that require Electronic Signature support can include Electronic Signature attributes: TDMX\_ES\_STATUS (Lookup) and TDMX\_ES\_DETAILS (Memo).

Use the Form Designer and Web Form Designer for adding these attributes.

---

**IMPORTANT!** Define these attributes as Read Only.

---

## Profile Cards of Admin Classes

Arrange profile cards to show added class attributes.

Verify that the ID Attribute includes Mask definitions, which are defined in the Setting Sequences for Administration Classes section in the SmarTeam – Job Server Administration Guide.

## Importing LDAP Users

**Note:** This section is for customers who are authenticated in LDAP instead of SmarTeam.

### **To import LDAP users:**

- 1 From the Admin Console, open the SmarTeam LDAP Users Import wizard.
- 2 Complete the relevant Server Information fields, such as the LDAP Server Address and LDAP Search Base fields. For additional details, see SmarTeam – Editor Online Help.

**Note:** Completing the Authentication Information fields is based on customer requirements and is optional.

- 3 From the LDAP Import Details window, complete all the fields for each user and click **Next**. The Import Results window appears showing a report of all the users who were imported.
- 4 Click **Finish**.

# Chapter 4: Electronic Signature

## Methodology

The purpose of the Electronic Signature is to ensure that the Released documents in the database are approved in a strict method that is implemented in the RCF. The Electronic Signature can be run in both SmarTeam – Web Editor and SmarTeam – Editor.

## Electronic Signatures Process Definition

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

The best practice is to manage the signing process in a SmarTeam Workflow Process so the logic is built via a SmarTeam workflow.

The administrator defining electronic signatures in the Flowchart Designer determines which nodes in the flowchart have electronic signatures and who can sign them.

**Note:** 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.

### Limitation

Objects of different super-classes cannot be attached to the same Workflow Process for Electronic Signatures. For example, to define Electronic Signatures for Items and Documents, two Workflow Processes must be used.

## Electronic Signatures Stages

Electronic Signatures include the following steps:

- **ES Configuration:** A technical user/manager specifies which documents from process attached documents need signatures and at which nodes the signatory can approve the document.

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

- **Signature:** The signatory signs and approves the documents, according to the rules defined by the technical user/manager. The signatory could be, for example, a Team Leader, a QA person, or a Documentation person.
- **Release:** If all signatures are complete, a task Releases all linked objects. If an object is a file managed, such as a document, the file update can be done using the Job Server.

## Electronic Signature Attributes

As part of the Electronic Signature mechanism, ES Details and ES Status attributes are added to the class, which an administrator can add to the profile card of objects signed with electronic signatures.

### ■ ES Details

Contains the following attributes:

- Process ID
- For each node that is signed: Node Name + Username (the one that signed) + Meaning of Signature + Date Time

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).

## Meaning of Signature

The Meaning of Signature attribute is a value the user completes when signing a process. This value is then added to the ES Details attribute.

This attribute can be defined by the administrator as free text/lookup for each Process/Electronic Signature node.

## Configurations

### Electronic Signatures Stages Implementation

For the Electronic Signatures steps there are three methods to run the signing scripts:

- Run as User Defined Tool (UDT) on the process
- Run from Task on the node
- Run when the workflow is accepted

This is the list of script by method:

Operation	Function Name	Method
ES Configuration	ESAdminUDT	UDT
	ESAdminWF	Before – Accept
	OnESAdminTask	Task
Signature	ESUDT	UDT
	ESWF	Before – Accept
	OnESTask	Task
	<Local Script> – see details below	Accept
Release	OnTasksStart	Task

#### LOCAL SCRIPT

If you create customized script functions for a signature that performs other operations before / after the signature, you must create an Admin Setting for each script to recognize this node as a signature node. Admin Setting format should be as follows:

- Section: **ES\_UPGRADE**
- Subject: **SIGN\_SCRIPT\_NAME**
- First Value: <Function Name>

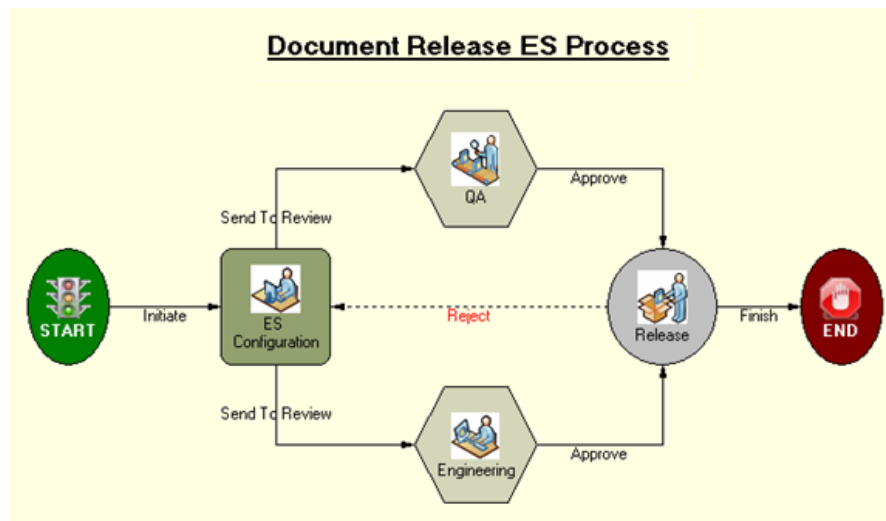
#### Notes:

- All RCF functions are located in the RegulatoryCompliance.ebs file (except Local Script option).
- For instructions about defining RCF User Defined Tools for Work in SmarTeam – Web Editor, see Appendix 1.
- If UDT is defined, you must create a menu item or an icon to run it. For more information on the Flowchart Designer, see SmarTeam – Editor Online Help.

## Configuring the Electronic Signature Workflow

This Workflow configuration, which is only a sample, shows how to define the Electronic Signature scripts on Before Send Accept of the workflow.

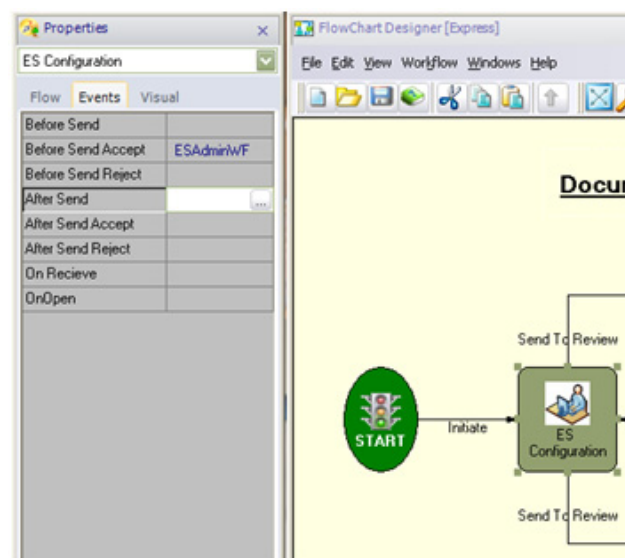
To configure the Electronic Signature Workflow, open the Flowchart Designer from Admin Console and create a workflow as shown in the following image.



### ES Configuration Node

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

- 1 Double-click the ES Configuration node to open the Properties window.
- 2 In the Before Send Accept event, hook the ESAdminWF function.

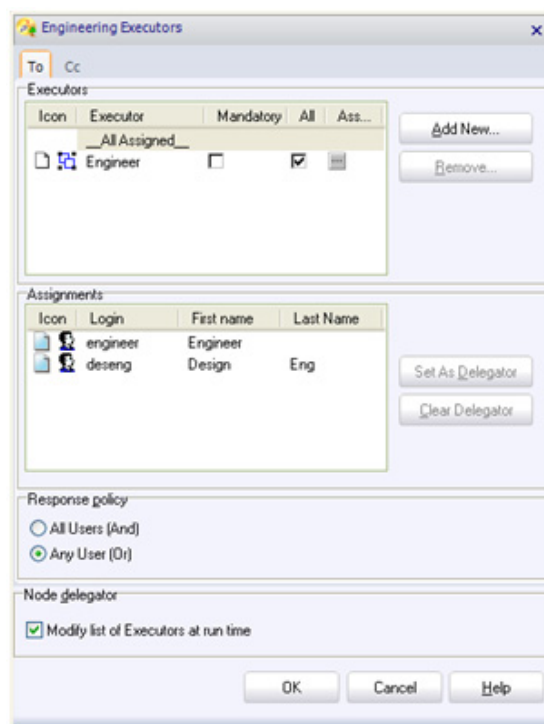


### Signature Nodes

You need at least one node for a signature. This example shows the creation of a QA node and an Engineering node.

- 1 Double-click on a **QA** node to open the Properties window.
- 2 In the **Before Send Accept** event, hook the **ESWF** function.
- 3 Define a Signatories and Response Policy by doing the following:

- a Double-click on the node.  
The node Executors window appears.
  - b From the Properties window, select the Flow tab, and click the Browse button in the 'To' field.
  - c Define groups/users for the node if they are always the same.
  - d Select Modify list of Executors at runtime to allow ongoing changes of node users.
  - e In the Response Policy area, select a response policy according to the requirements for this Electronic Signature. This setting determines what appears on the ES Configuration node:
    - All Users (And) includes two values: All/None
    - Any User (Or) includes two values: One/None
  - f None: ES Configuration node user can define that a specific document does not need to be signed.
- 4 Repeat this operation for **Engineering** node.



### Node for Release

Set up the release of the documents after all the documents have been signed.

#### ■ Reject

- 1 Double-click on a Release node to open the Properties window.
- 2 In the Before Send Reject event, hook the DeleteAllSignaturesOnProcessEx function.
- 3 This script deletes signatures on signed objects that are attached to the process.

#### ■ Release the Documents

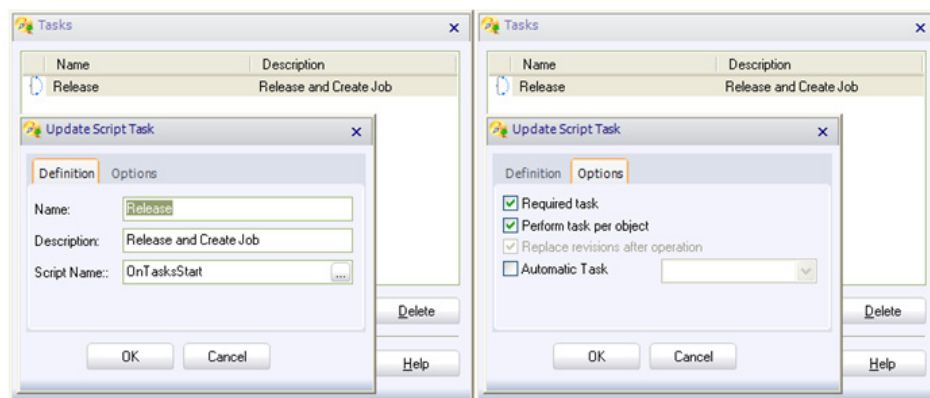
- 1 Double-click on a Release node to open the Properties window.
- 2 Add Script Task, hook the OnTaskStart script.



- a** This script checks if all signatures are completed and if so, all linked objects are be released.
- b** If an object is file managed, such as a document, Job Server can update the file.
- c** This is done by hooking CreateJobBasedOnFileType to the After stage of the Release operation.
- d** This script adds a Job in the queue of the Job Server.  
For additional details about the Job Server, see the SmarTeam – Job Server Administration Guide.

**Note:** If you define Audit Trail as well, you must merge the scripts or call the Audit Trail from the script of the Electronic Signature.

- 3** Optional: In the Options tab, define the task to be automatically performed on the capture. If so, make sure that the user does not have the option to reject the workflow process from this node.



**Note:** For more information on the Flowchart Designer, see SmarTeam – Editor Online Help.

## Define Meaning of Signature Attributes

This attribute can be defined by the administrator as free text/lookup for each Process/Electronic Signature node.

You must define Admin Setting for each process/node in the process in the following format:

- 1** Section Attribute = MeaningOfSignatureDefinition
- 2** Subject = <Flowchart Name>\_<Node Description> where:
  - a** Flowchart Name: Name of the flowchart for which the Meaning of Signature is defined.
  - b** Node Description: Name of the node for which the Meaning of Signature is defined (optional).
  - c** If a Node Description is not specified the definition is applied to all the nodes in the flowchart.
- 3** Long Value Attribute:
  - a** For Lookup: Lookup values delimited by semicolons: <value1>;<value2>;<value3>.

For example, Approve;Confirm;Reject

- b** For Free Text: Leave this field blank.

## Other Scripts of Electronic Signature

In the RegulatoryCompliance.ebs script file there are more functions that complete the scenario of Electronic Signature.

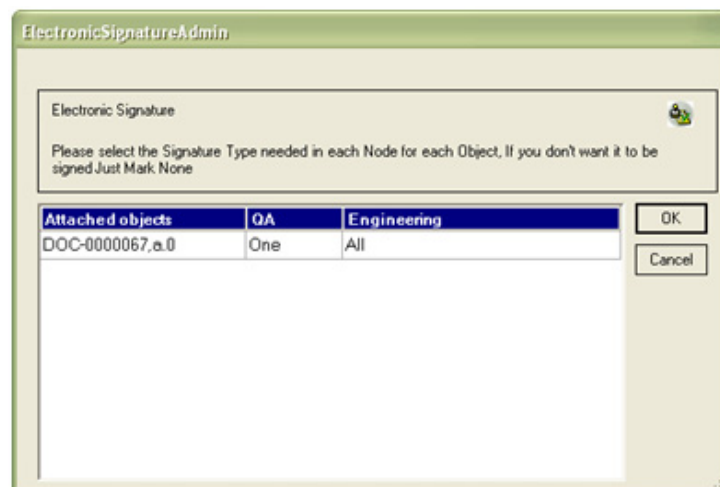
Function Name	Operation	Hooks	Description
CheckObjectSignedBefore-update	Update	Before	Stop the update operation if object has at least one signature.
CheckObjectSignedOnStartup	Screen Startup	On	Stop the update operation if object has at least one signature.
DeleteAllSignaturesOnObject	Check Out, New Release, Add as Copy	After	Deletes signatures on selected signed objects.
GetAllSignaturesOnObjectEx	UDT		Get signatures details on selected objects as record list.

## How to use an Electronic Signature

The following is a full scenario the user must perform to sign documents in the sample process defined in the previous section.

- 1** Create new approval process:
  - a** Initiate the process.
  - b** Attach the required documents to this process.
  - c** Define the user for the ES Configuration node if it is not defined in the workflow.
  - d** Select Accept to move to the next node.
- 2** ES Configuration node:
  - a** The documents presented in the signature window are:
    - Attached to the process.
    - 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.
  - b** Select Accept to show the Electronic Signatures Admin window (since in this example the configuration is hooked to Accept).
  - c** Only the nodes with an Electronic Signature appear:
    - The script reviews all nodes in the flow process, checks which nodes have Electronic Signature script attached and displays all the nodes on the GUI. For each node, one column appears.
    - In this example the QA and Engineering nodes have Electronic Signatures.

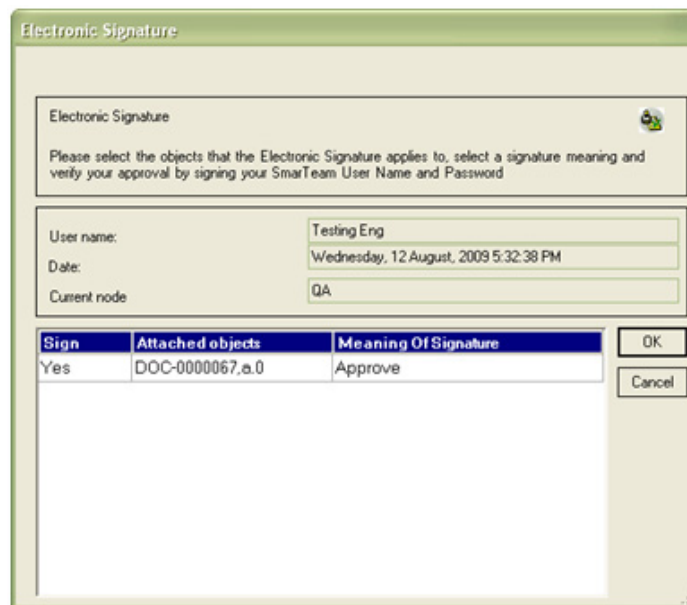
- d** Select if each document should be signed (corresponding to definition in the Response Policy) as follows:
  - For 'OR' policy select one of the options:  
 One: Only one signatory needs to sign this document (default).  
 None: No signatories need to sign this document. If this option is selected, the document does not appear in the list of documents seen by the signatory.
  - For 'AND' policy select one of the options:  
 All: All signatories need to sign this document (default).  
 None: No signatories need to sign this document. If this option is selected, the document does not appear in the list of documents seen by the signatory.
- e** Before selecting, you can view the Profile Cards of the documents listed in this window by clicking on their links on the Attached Objects column.
- f** You cannot finish the Accept before configuring the Electronic Signatures. If you select Cancel before completing the configuration process, the Configuration window appears again next time you click Accept on the process.
- g** If the number of users who need to sign changes, these changes must be reflected in a node after approving the Electronic Signatures Admin window. The Electronic Signatures Admin window must be run again. If the process was already promoted to next nodes, the process needs to be rejected to the ES Configuration node.



### 3 Signature Nodes

- a** Signatory check the documents before signing
- b** Select Accept to show the Signature window (since in this example the configuration is hooked to the Accept).
- c** Signing window:
  - In the Electronic Signature window, select the Sign checkbox for each document you want to sign.
  - The Username, Date and Current Node fields are disabled and therefore cannot be changed.

- Before signing documents, you can view the Profile Cards of the documents listed in this window by clicking on their links.
- Select an option from the Meaning of Signature list or type in the meaning of the signature in this field, and click OK.



**Electronic Signature**

Electronic Signature

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

User name: Testing Eng

Date: Wednesday, 12 August, 2009 5:32:38 PM

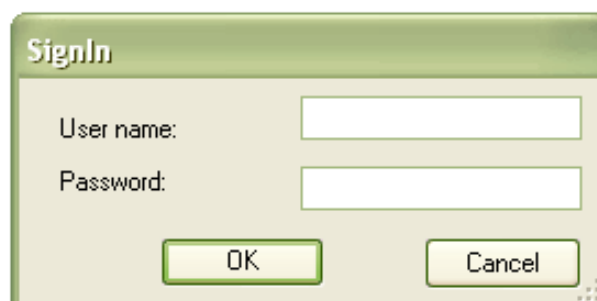
Current node: QA

Sign	Attached objects	Meaning Of Signature
Yes	DOC-0000067.a.0	Approve

OK Cancel

- d** In the Electronic Signature Validation dialog box, type your Username and Password and click **OK**.

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



**SignIn**

User name:

Password:

OK Cancel

- e** You cannot finish the **Accept** before configuring the Electronic Signatures. If you select **Cancel** before completing the configuration process, the Configuration window appears again next time you click **Accept** on the process.

# Chapter 5: Audit Trail

## Methodology

The purpose of the Audit Trail is to supervise the following activities of SmarTeam users: Add, Update, Delete, Lifecycle operations and Login of the user to the system. These activities are saved in the database and can be viewed by the administrator via a dedicated tool. The Audit Trail can be run in both SmarTeam – Web Editor and SmarTeam – Editor.

## Configuration

The following are the relevant configurations for Audit Trail.

### Audit Trail Script

Audit Trail functionality is performed by attaching scripts on Before and After hooks for selected operations. Use the Script Maintenance from the Admin Console to define the scripts.

Audit Trail scripts can be configured in two hooks:

Hook	Function	Function Description
Before	SaveToGlobal	Save parameters of the object to memory (global data) before the operation runs to compare it after the change.
After	AuditTrail	Creates a new Audit Trail record If a saved object is in memory, the function compares the current values of the records with the saved record and writes the differences in the Description field.

#### Notes:

- Both functions are located in the RegulatoryCompliance.ebs file.
- If you define Audit Trail as well, you must merge the scripts or call the Audit Trail from the script of the Electronic Signature.

## Audit Trail Supported Hooks and Classes

To configure to view Audit Trail hooks, open the Script Maintenance from the Admin Console and configure hooks as described in the following table.

Type	Class	Operation	Hooks
Login Process	Class Browser	OnUserAuthentication	After
Managed Classes	e.g., Projects, Documents, Items	Add	After
		Update, Delete	Before & After
	e.g., Documents	Lifecycle Operations: Check in, Check out, Release, New Release, Obsolete	After
Link Classes – Hierarchical links and relation links (one-level links)	e.g., Document Tree	Add	After

**Note:** Item Lifecycle is not supported.

## Audit Trail Hooks for Internal Classes

By running the RCF Admin Setup the following operations occur:

- 1** Add HSysManager, SmarTeam internal user to handle errors when the login process fails.
- 2** Attach scripts for the Audit Trail on internal classes:
  - a** Users: SmarTeam Users (Add, Update and Delete)
  - b** Authorization Group: SmarTeam Groups (Add, Update and Delete)
  - c** User Relation to Group: Association of SmarTeam Users to SmarTeam Groups (Add, Update and Delete)
  - d** TDMX Signature: Electronic Signatures (Add, Update and Delete)
  - e** User Authorization: Authentications of SmarTeam Users and SmarTeam Groups (Add and Delete)

## Merging Scripts

When more than one script is required to run from the same hook, you must merge the scripts.

For example, there is a PLMDB\_ObjectInitialization script hooked on Before Add operations. To perform an audit trail to the Add activity, you must merge the ObjectInitialization script with the Audit Trail script.

## Enabling the Viewing of Audit Trail Records

### *To configure to view Audit Trail records:*

- 1 From the Admin Console define UDT:
  - a Open the Script Maintenance.
  - b Switch to the User Defined tab.
  - c Select Class Browser in Class Tree.
  - d Add an operation, such as Audit Trail Query.
  - e Attach the AuditTrailQuery script.
- 2 Define Menu:
  - a Open the Menu Editor.
  - b Create a menu item or an icon to run the Audit Trail command.
- 3 Add Permissions:
  - a Open User Maintenance.
  - b Define permissions for the Administrator to run this tool.

**Note:** For instructions about how to define RCF User Defined Tools (UDT) for Work in SmarTeam – Web Editor, see Appendix A.

## How to use Audit Trail

### *To view Audit Trails:*

- 1 Open the Audit Trail Query window by running the UDT.
- 2 In the Filter Options area (top of window) you can define to filter the results as follows:
  - a Data From: All records to which the date is equal or after the selected date.
  - b Data To: All records to which the date is equal or before the selected date.

**Note:** When opening the Audit Trail screen, the Date From and Date To fields are populated with the current date. To launch a query, the user must set the correct criteria for these dates.

- c Username: All records performed by a specific user.
- d Computer Name: All records made at a specific computer.

- 3 For advanced filter options, click the + button on the right side of the window in the Filter Options area. The following options appear:
  - a Operation: List of all operations that can be trailed
  - b Alert: Normal or Critical
  - c NT Username: Network user login name
  - d Audited ID: Selected object

**Note:** The contents of this field cannot be changed, only cleared.
- 4 Clear: Clear all Filter Options:
  - a Date From and Date To are set to today.
  - b All other options cleared including selected object that is completed by default.
- 5 Run: Run the query according to the filter definitions.
- 6 After the Audit Trail is run, the following data appears:
  - a ID: Particular Audit record's ID.
    - i. When creating an Audit record, first a search is done for the user defined sequence in the ID attribute of the Audit Trail Class (Preferred).
    - ii. If a sequence is not defined by the user, the generated ID is the current date and time according to the following format: Year, Month, Day, Hour, Minute, Second.
  - b Date: Date on which the operation occurs.
  - c Username: SmarTeam Username that triggered the Audit Trail creation. It may be the logged in user or an internal user.
  - d NT Username: Network user login name. Because a regular user (not an Administrator) must log in with the same username as the network login name, this value differs from the Username field only for a user who logs in as an Administrator.
  - e Computer Name: The computer name from which the user logged on.
  - f Operation: The operation that triggers the Audit Trail, such as Add, Update, Delete or Release.
  - g Alert: Alert type:
    - i. Critical: For Delete operation.
    - ii. Normal: For other operations.
  - h Audited ID: Audited object primary attribute.
    - i. If a document is audited, this field contains a document identifier (Doc-0095, etc).
    - ii. If a user login is audited, the username that is audited appears.
    - iii. If user login fails, the system creates a record with help of the HSysManager internal user. Hence, this record's Audited ID is HSysManager.
  - i Description: The description of the Audit Trail record. The description records operations and changes.
- 7 When selecting a row from the results, the Record Full Details area is presented with the following options: ID, Description, Date, Username, Computer Name, Alert, Operation and NT Username.



- 8 Sort Results: When clicking on one of the headers of the table, the results are sorted according to the column.
- 9 Export to excel: Export the results to an Excel file.

**AuditTrail Query**

**Filter Options:**

☒ Date From: 09/Aug/2009 User name: [ ] Run [ ]

Date To: 13/Aug/2009 Computer name: [ ] Clear [ ]

Operation: [ ] NT User Name: [ ]

Alert: [ ] Audited ID: [ ]

Export to excel [ ]

ID	Date:	Username	NT	Computer	Operation	Alert	Audited ID	Description
2009Aug1311534	13/08/2009 11:53:4	Admin .	zgb	ILTDM120	Delete	Critical		Delete Main c
2009Aug1311525	13/08/2009 11:52:5	Admin .	zgb	ILTDM120	Login	Normal	admin	'Login'.User :'
2009Aug1311502	13/08/2009 11:50:2	Admin .	zgb	ILTDM120	Login	Normal	admin	'Login'.User :'
2009Aug1311493	13/08/2009 11:49:3	Admin .	zgb	ILTDM120	Login	Normal	admin	'Login'.User :'
2009Aug1301033	13/08/2009 1:03:32	Admin .	zgb	ILTDM120	Delete	Critical		Delete Main c
2009Aug1205365	12/08/2009 5:36:56	Design .	zgb	ILTDM120	Electronic signature	Normal		The object D
2009Aug1205362	12/08/2009 5:36:30	Design .	zgb	ILTDM120	Login	Normal	deseng	'Login'.User :'
2009Aug1205355	12/08/2009 5:35:58	Compon	zgb	ILTDM120	Electronic signature	Normal		The object D
2009Aug1205355	12/08/2009 5:35:58	Compon	zgb	ILTDM120	Electronic signature	Normal		Electronic sig
2009Aug1205353	12/08/2009 5:35:30	Compon	zgb	ILTDM120	Login	Normal	compeng	'Login'.User :'
2009Aug1205345	12/08/2009 5:34:55	Engineer	zgb	ILTDM120	Electronic signature	Normal		The object D
2009Aug1205345	12/08/2009 5:34:55	Engineer	zgb	ILTDM120	Electronic signature	Normal		Electronic sig
2009Aug1205335	12/08/2009 5:33:58	Engineer	zgb	ILTDM120	Login	Normal	engineer	'Login'.User :'

Record Full Details

**Note:** To enable exporting of Audit Trail records in 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.

# Chapter 6: Enhanced User Security

## Configuration

To enable enhanced security, configure the SmarTeam – Job Server and configure the Mail Executable for the SmarTeam – Job Server.

For information about setting up the SmarTeam – Job Server, see the Job Server Administration Guide.

## Admin Settings

The Admin Settings are used by the system administrator to specify default settings for the various jobs performed by means of the SmarTeam – Job Server.

Admin Settings are presented in table format. In each table, the following topics are presented, when relevant:

- Section
- Subject
- First Value
- Second Value
- Third Value
- Fourth Value
- Long Value

**Section** and **Subject** are identifiers for the Admin setting described within the table. The values (**First**, **Second**, etc.) define the value to be used in the particular setting.

## General Settings

Define name of Administrator to receive email notification of errors		
Attribute Name	Value	Description
Section	FDA Settings	Identifiers for the Admin setting
Subject	Admin	
First Value	<Admin user name>	The user name of Administrator, for example, <b>Admin</b> , who is informed by email about low-level errors, e.g., Audit trail errors
Second Value	<Admin user name>	The user name of Administrator who is informed by email about high-level errors, e.g., login failure errors

## Harden User Security

Default creation of SmarTeam users does not include password restrictions.

### Minimum Password Length

All SmarTeam users must have a password of minimum length. This requirement is customized in SmarTeam – Editor by the administrator.

All users must therefore reconfigure their passwords at least to the minimum length that the administrator determines. Users can change their passwords in the User Maintenance or during the next login if the administrator defines the passwords as expired.

Administrator must verify that all users have passwords according to the minimum required length.

#### ■ Password Configuration

- 1 In the User Maintenance, for each existing user:
  - a Configure the password in accordance with company requirements (Minimum Password Length and Complexity Requirements if selected).
  - Or  
Set Password Expiration Date to today so the user must replace the password. Verify all users change their passwords in accordance with company requirements.
  - b Password Algorithm must be md5.
  - c Check that the following attributes are defined: First Name, Last Name, Email and Phone.
- 2 Log in to SmarTeam – Editor as an Administrator.
- 3 From Administrator Options select User Account Options.
- 4 Under the General tab, change the Account lockout threshold to 3.
- 5 Under the Password tab, configure the Password Policy:
  - a Minimum Password Length to at least 6.

- b** Minimum Password Length to 10.
  - c** Minimum Password Length to 90.
  - d** Select Password must meet complexity requirements checkbox.
- 6** Under the Password tab, deselect the Allow Plain text checkbox.

---

**IMPORTANT!** Before deselecting the Allow Plain text checkbox, you must be absolutely certain that the Administrator password meets the defined password requirements. If the password requirements are not fulfilled completely, the Admin account will be locked out.

---

**Note:** All values above are standard recommendations. The Administrator can change them according to company policy.

## New User Creation

When an administrator creates a new user, the following occurs:

- The user is created in an Inactive state. After the user is created, the Inactive checkbox can be deselected.
- 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 Option 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.

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.

# Appendix A: Define RCF User Defined Tools for Work in SmarTeam – Web Editor

## *To run the RCF events from User Defined Tool:*

- 1** Open the configuration file for editing: SmarTeam\Configuration Settings\Data\Domain\smarteam.std.webEditor.config.xml.
- 2** If the smarteam.std.webEditor.config.xml file does not exist in the Domain level, do the following:
  - Copy the xml file from the Default level to the Domain level.
  - Clear the content of this file and maintain the configuration code.
- 3** Add the User Defined Tool keys.
- 4** The Operation Name must be the same as the name in the Script Maintenance.

### Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns="http://www.smarteam.com/dev/ns/config/webEditor/1.0"
xmlns:cs="http://www.smarteam.com/dev/ns/config/1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLoca-
tion="http://www.smarteam.com/dev/ns/config/webEditor/1.0 http://www.smart-
eam.com/dev/schema/config/webEditor/1.0/webEditor.xsd">
  <userDefinedTools>
    <userDefinedTool>
      <operationName>ES Configuration</operationName>
      <pageName>SmarTeam.Solutions.ElectronicSignature.Web.GUI/ElectronicSignatureAd-
min.aspx</pageName>
    </userDefinedTool>
    <userDefinedTool>
      <operationName>Signature</operationName>
      <pageName>SmarTeam.Solutions.ElectronicSignature.Web.GUI/ElectronicSigna-
ture.aspx</pageName>
    </userDefinedTool>
    <userDefinedTool>
      <operationName>AuditTrailQuery</operationName>
      <pageName>SmarTeam.Solutions.AudiTrail.GUI.Web/AuditTrailQuery.aspx</pageName>
    </userDefinedTool>
  </userDefinedTools>
</configuration>
```

## Appendix B: RCF Internal Classes

The RCF mechanism added several internal classes for the use of the RCF functionality. The following is a list of the internal classes.

### Electronic Signature

- TDMX\_SIGNATURE:
  - Contains the signature for all objects.
  - When the ES Configuration function runs it completes the signatures needed for the process attached objects.
  - All functions that search for the signatures of an object work with this table.
  - This table includes attributes that link to the Workflow Node, Object, Signee, Date Time and Meaning of Signature.
- TDMX\_ES\_STATUS\_VALUES: Values of Electronic Signature Status

### Audit Trail

- TDMX\_AUDIT\_TRAIL
  - Contain all the operations recorded in the database via configuration.
  - This table is used in the Audit Trail Query to view the results with the filter definitions.
- TDMX\_AT\_ALERT: Values of Audit Trail Alert.
- TDMX\_AT\_OPERATION: Values of Audit Trail supported operations.

## Appendix C: RCF Upgrade Mechanism

This Upgrade Procedure describes how to upgrade from SmarTeam Database in R17 SPx (before SP6) with FDA mechanism to RCF and Job Server in SmarTeam R19 SP6.

### Upgrade Process

#### *To perform and update:*

- 1 Exit all SmarTeam application.
- 2 Back up your database.
- 3 Back up the SmarTeam environment.
- 4 Validate that Office Interops (Microsoft.Office.Interop.Excel, Microsoft.Office.Interop.Word) for Office 2003 exist and are registered. If not, download and register Microsoft® Office XP primary Interop assemblies (PIAs). For additional information, see:  
<http://www.microsoft.com>.
- 5 Detach the scripts hooked on **On Authentication** using the Script Maintenance tool.
- 6 Remove ENOVIA SmarTeam software.
  - a Uninstall ENOVIA SmarTeam Applications.
  - b Delete remaining files and folders.
  - c Clean the registry from keys if any remain.
- 7 Install R19 SP6 or above.
- 8 Review the next section: [Database Preparations](#).
- 9 If the database includes a script that can prevent the DMD from running, disable this script.
- 10 Run DMD and verify that the following mechanisms are selected:
  - a Audit Trail
  - b Electronic Signature
  - c Job Server
- 11 Click **Create** to run the DMD.
- 12 During the checking data model step, there is a test to verify if the change in the FDA will run correctly.
- 13 If the FDA will not run correctly, an error message appears referring to a log file. The log file includes information about problematic objects in the database. If this occurs, do the following:
  - a Based on this information, write an SQL script to fix these objects.

- b** Run this SQL script on the database.
- c** Click **Create** again.
- 14** Verify that **HSysManager** user is a member in the Administrator's group.
- 15** Run **SmarTeam.Solutions.RegulatoryComplianceSetupAdministrator.Exe**.
- 16** Run the DMD again and remove the FDA support (obsolete) mechanism (first window).
- 17** New RCF scripts must be copied from the SmarTeam SDK folder to the Scripts folder.
- 18** Change the hooked scripts in the script maintenance to the new Regulatory Compliance scripts.
- 19** Update the Admin settings according to the RCF requirements.

## Database Preparations

After the first time you run DMD, new Admin Settings are defined with the issues that occur in the upgrade process. You need to analyze these settings and fix the database before running the DMD again.

The following are samples for known problems:

**Problem:** Username (First Name or Last Name) of the user was changed.

**Solution:** Change the signatures in the database to the new Username.

**Problem:** First Name and Last Name are equal.

**Solution:** Change one attribute: First Name or Last Name.

**Problem:** If **TDM\_ES\_BY\_1** exists and **TDM\_ES\_DATE\_1** or **TDM\_MEANING\_OF\_SIGNATURE** are empty or not in the correct format the signature is not created in the new format of the signature.

**Solution:** Verify **TDM\_ES\_DATE\_1** and **TDM\_MEANING\_OF\_SIGNATURE** are completed in the correct format.

**Problem:** If a user changes the error messages (Admin Super Class) a problem may occur in the upgrade.

**Solution:** Change the error messages back to the original messages.