



# Proficiency Batch Execution 5.6

## Electronic Signatures and Auditing



**Proprietary Notice**

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2020, General Electric Company. All rights reserved.

**Trademark Notices**

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

[doc@ge.com](mailto:doc@ge.com)

# Table of Contents

About This Guide .....	1
Reference Documents .....	1
Introduction to Electronic Signatures .....	1
What are Electronic Signatures? .....	2
Types of Electronic Signatures .....	2
Overview of Where You Can Use Electronic Signatures .....	3
Additional Constraints for Electronic Signatures .....	4
The Same User Cannot Sign the Performed By and Verified By Signatures.....	4
The Performed By and Verified By Users Must Have a Full User Name Defined .....	4
The Performed By and Verified By Users Must Have Different Full User Names .....	5
What Determines a Signed Action?.....	5
Actions Available for Signing in the Recipe Editor .....	5
Actions Available for Signing in the Equipment Editor .....	6
Actions Available for Signing in the ActiveX Controls .....	6
Actions Available for Signing in the Audit Reporter .....	8
Actions Available for Signing in the Batch Execution Configuration .....	8
Tracking Electronic Signatures.....	9
Understanding 21 CFR Part 11 .....	10
Using 21 CFR Part 11 Services from GE Intelligent Platforms .....	10
Understanding Windows Security and Electronic Signatures .....	10
Using Local and Domain Groups.....	11
Example for Configuring Windows Security .....	11
Adding Operators and Supervisors .....	11
Overview of Windows Security Groups .....	12
User Created Windows Security Groups.....	12

Batch Execution Created Windows Security Groups .....	12
Additional Considerations When Creating User Accounts .....	13
Specifying the Full User Name .....	13
Specifying the Number of Invalid Signature Attempts .....	13
Setting the Password Expiration for Users Performing Electronic Signatures .....	13
Tracking Invalid Signature Attempts with Windows Auditing .....	14
Disallowing Blank Passwords .....	14
Disabling the Ability to Change the System Time .....	14
Other Considerations .....	14
Configuring Electronic Signatures .....	14
Overview for Configuring Electronic Signatures .....	15
License and Key Checking .....	15
Configuring Electronic Signatures for the Recipe Editor, Equipment Editor, and the Batch Execution Configuration .....	16
Understanding iFIX Security and Batch Execution Electronic Signatures .....	18
Configuring Electronic Signatures for the ActiveX Controls .....	19
Configuring Electronic Signatures for the Audit Reporter .....	20
Performing Electronic Signatures .....	21
Example of Electronic Signature Dialog Box .....	21
What Happens if the Signature Fails? .....	22
Examples of Electronic Signatures .....	22
Performed By Signature .....	22
Performed By/Verified By Signature .....	23
Comments with an Electronic Signature .....	24
Performed By Signature in the ActiveX Controls .....	24
Performed By/Verified By Signature in the ActiveX Controls .....	25
Examples of Failed Signing Attempts .....	25
Invalid User Name or Password .....	25

Account Expired.....	26
User Not a Member of the Required Group .....	26
The Same Full User Name Not Accepted for Both Signatures .....	26
The Same User Cannot Sign Both Signatures.....	27
Electronic Signature Request Cancelled from the Audit Reporter .....	27
Security Group Does Not Exist on the Domain .....	27
Understanding Audit Versioning and the Audit Trail.....	28
Automatic Versioning of Area Models and Recipes .....	28
What is Captured with the Audited Document?.....	29
Viewing the Design-time Audit Information.....	31
Example of Viewing Design-time Audit Information .....	32
Using the Audit Reporter to View the Audit Trail.....	32
What Types of Data Does the Audit Trail Store? .....	33
Viewing Audited XML Documents .....	34
Example of an XML Schema .....	34
Enabling Auditing.....	35
Configuring Auditing in the Batch Execution Recipe and Equipment Editors .....	36
Configuring Auditing in the Audit Reporter .....	36
Using Auditing Without Capturing Signatures .....	36
Determining if a Batch Execution Project or Recipe Has Auditing Enabled.....	37
Monitoring Product Baselines with Audit Information .....	37
Auditing Database Tables .....	38
BATCH_AUDIT_INFO Table.....	39
AUDITTABLE Table.....	47
AUDITREPORTTEMPLATES Table .....	54
Example of an Audit Trail .....	54
Action 1: Startup .....	55
Action 2: Open .....	55

*Electronic Signatures and Auditing*

Action 3: New.....	55
Action 4: Print .....	55
Action 5: Remove Recipe .....	56
Action 6: Release to Production .....	56
Action 7: Rebuild a Recipe Directory.....	56
Action 8: Save a Recipe Without Verifying.....	57
Action 9: Save a Recipe, Accept and then Cancel the Verification of the Electronic Signature .....	57
Action 10: Save and Verify a Recipe .....	57
Action 11: Verify but Not Save a Recipe .....	58
Action 12: Verify and Save a Recipe .....	58
Action 13: Verify All Recipes .....	58
Action 14: Save As .....	58
Action 15: Convert Project Storage and Cancel the Electronic Signature .....	59
Action 16: Convert Project Storage and Accept the Electronic Signature.....	59
Action 17: Upgrade Recipes and Cancel the Electronic Signature .....	59
Action 18: Upgrade Recipes and Accept the Electronic Signature .....	59
Audit Reporter Dialog Boxes .....	60
Data Source Configuration Dialog Box.....	60
Datasources Dialog Box .....	61
Electronic Signature Dialog Box .....	61
Page Setup Dialog Box .....	61
Report Template Dialog Box .....	62
How Do I.....	64
Shortcuts in the Audit Reporter .....	65
Performing Basic Operations in the Audit Reporter .....	65
Working With Reports.....	70
Running Reports.....	75

Modifying Report Viewing Formats.....	77
Modifying Report Display Options .....	78
Printing Reports .....	81
Optimizing Reports .....	82
Index .....	87



---

## About This Guide

This manual provides an overview of GE's electronic signature feature in the Proficiency Batch Execution product. This manual addresses the needs of application developers and process control engineers who want to incorporate electronic signatures and secure electronic records (security audit trails) in their Batch Execution operations.

---

## Reference Documents

For related information about subjects discussed in this manual, refer to these manuals:

- System Configuration Manual
- WorkInstruction Manual

---

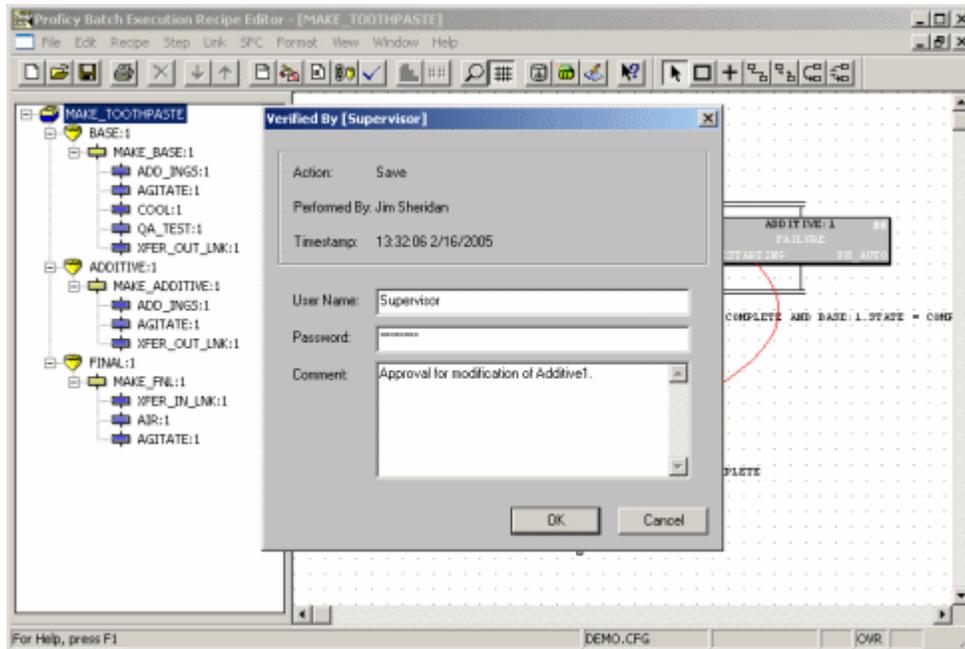
## Introduction to Electronic Signatures

GE originally introduced electronic signatures with the WorkInstruction product. The Batch Execution product also includes the electronic signature capability in most ActiveX Controls, in the Batch Execution Recipe Editor and Equipment Editor (when used through the Batch Execution WorkSpace or launched independently, outside of the WorkSpace), in the Electronic Signature page in the Batch Execution Configuration, and in the Audit Reporter application.

With electronic signatures enabled, you can provide user authentication prior to the execution of a Batch Execution command. For example, the types of commands (actions) you can authenticate against in the Batch Execution Editors include Startup, Open, Save, Save As, Print, Export, and Verify.

All signatures are authenticated using Windows security. This means that an operator must enter a valid user name and password from a Windows security group to complete the command. You must create these groups and users with your Windows software. Once created, you assign the commands and groups that you want to authenticate against when configuring your Batch Execution software.

The following figure shows an example of the Verified By Electronic Signature dialog box in the Recipe Editor. In this example, the Recipe Editor requests a Verified By signature to perform the Save command. A Performed By signature has already been entered. You will notice the name of the command and the full user name of the user who entered the Performed By signature in the unavailable fields above the Verified By signature request fields. A time stamp displays the date and time when Batch Execution authenticated the electronic signature of the operator in the Performed By group.



Electronic Signature Example in the Recipe Editor

This section presents an overview of the tasks required to implement and use the Electronic Signature option.

---

## What are Electronic Signatures?

Electronic signatures are the computer-generated, legally-binding equivalents of handwritten signatures. They uniquely identify the person(s) responsible for an action.

An electronic record is generated each time an action is signed for in the Batch Execution and WorkInstruction products. Electronic records consist of the name of the person(s) involved in the signing process, and other details, such as the type of action performed and a user comment. Electronic records are written to a relational database, and retained as a permanent record of a signed action.

## Types of Electronic Signatures

The signature requirements that you select define whether or not a user or users must "sign-off" on a command before it is performed. You can define the following signature types for each Batch Execution action:

- None (no signature required)
- Performed By (only "Performed By" signature required)
- Performed By/Verified By (both "Performed By" and "Verified By" signatures required)

If you do not select a signature type, no signature is requested when you perform the action; None is the default signature type. If you do not want to define these signature types for each action individually, you can specify one signature type for all actions by using the default signature option.

For example, the following figure shows how you configure the Electronic Signature tab in the Batch Execution Configuration so that None is the default signature type for the Recipe Editor, and that Performed By is the default signature type required for the Equipment Editor. Electronic signature configuration is defined in more detail in the Configuring Electronic Signatures section.

The screenshot shows two panels: 'Recipe Editor' and 'Equipment Editor'. Each panel has a checked checkbox for 'Use Default Signature Requirements' and a table with four columns: 'Command', 'Signature Requirements', 'Performed By', and 'Verified By'.

Command	Signature Requirements	Performed By	Verified By
<b>Default</b>	<b>None</b>		
Convert Project Storage	None		
New	None		
Open	None		
Print	None		
Rebuild Recipe Directory	None		
Release To Production	None		
Remove	None		

Command	Signature Requirements	Performed By	Verified By
<b>Default</b>	<b>Performed By</b>	<b>Operator</b>	
Export	None		
Import	None		
New	None		
Open	None		
Print	None		
Save	None		
Save As	None		

*Example of Using the Default Signature Requirements in the Recipe and Equipment Editors*

## Overview of Where You Can Use Electronic Signatures

The following Batch Execution components support electronic signatures:

- Batch Execution Recipe Editor
- Batch Execution Equipment Editor
- Batch Execution Workspace (when used as a container for the Equipment Editor)
- Batch Execution Audit Reporter
- Batch Execution ActiveX Controls
- WorkInstruction Editor
- Electronic Signature page in the Batch Execution Configuration (when launched independently or through the Batch Execution Workspace)

The Configuring Electronic Signatures section describes how to configure and use electronic signatures in the Batch Execution applications. For information about configuring and using electronic signatures in the WorkInstruction Editor, refer to the WorkInstruction Manual.

The following figure shows an example of the Electronic Signature dialog box in the BatchList ActiveX control. This example shows the Verified By Electronic Signature dialog box that displays after you enter a Performed By signature for the Add Batch command. Note that the title bar of the dialog box lists the security group that the user must be a member of to enter the electronic signature. In the following figure, the dialog box requests a signature from the Supervisor group.



*Electronic Signature Example in the BatchList ActiveX Control*

---

## Additional Constraints for Electronic Signatures

This section describes constraints that Batch Execution and WorkInstruction enforce for a user signing an electronic signature.

### The Same User Cannot Sign the Performed By and Verified By Signatures

The same user cannot sign both the Performed By and Verified By signature for the same command, even if that user resides in both the Performed By and Verified By groups. What that means, is that the user performing a command cannot be the same user as the one who verifies that command.

### The Performed By and Verified By Users Must Have a Full User Name Defined

Although Windows security allows user accounts to be created without a full user name defined, you must define a full user name if you want to give a user the ability to sign for actions. Batch Execution and WorkInstruction do not accept signatures without a full user name defined. By accepting only signatures with a full user name, you have a more complete way of recording and tracking user actions in the audit trail database.

## **The Performed By and Verified By Users Must Have Different Full User Names**

When an action requires two signatures (Performed By and Verified By signatures), the two accounts must have different full user names. Regardless of the location of the groups (local or domain), Batch Execution and WorkInstruction compare the full user name of both signatures. If the full user names match, even if the user names are different, Batch Execution or WorkInstruction won't accept the signatures.

---

## **What Determines a Signed Action?**

The prompt for an electronic signature when you perform an action is determined by the way you configure electronic signatures in each of the Batch Execution components that support electronic signatures. Each Batch Execution component has different actions to which you can assign signature types and Windows security groups.

The following sections describe the actions for which you can configure electronic signature requirements:

- Actions Available for Signing in the Recipe Editor
- Actions Available for Signing in the Equipment Editor
- Actions Available for Signing in the ActiveX Controls
- Actions Available for Signing in the Audit Reporter
- Actions Available for Signing in the Batch Execution Configuration

For information on configuring actions for signing in the WorkInstruction editor, including all document management system (DMS) functions, refer to the WorkInstruction Manual.

## **Actions Available for Signing in the Recipe Editor**

You can configure the following actions to require electronic signatures in the Batch Execution Recipe Editor:

- Converting the project storage type
- Creating a new recipe
- Exporting a recipe
- Opening a recipe
- Printing a recipe
- Rebuilding a recipe directory
- Releasing a recipe to production
- Removing a recipe
- Saving a recipe
- Saving a recipe under a new name (Save As)
- Starting the Recipe Editor

- Upgrading a recipe
- Verifying a recipe
- Exporting a recipe
- Saving a formulation
- Removing a formulation
- Changing a formulation status

## **Actions Available for Signing in the Equipment Editor**

You can configure the following actions to require electronic signatures in the Batch Execution Equipment Editor, whether you launch the Equipment Editor independently or from the Batch Execution WorkSpace:

- Exporting an area model from the Equipment Editor
- Importing an area model into the Equipment Editor
- Creating a new area model
- Opening an area model
- Printing an area model
- Saving an area model
- Saving an area model under another name (Save As)
- Starting the Equipment Editor
- Upgrading an area model

## **Actions Available for Signing in the ActiveX Controls**

You can configure the Batch Execution ActiveX Controls to require electronic signatures for the actions listed for each command, as described in the following section.

### **BatchList ActiveX Control**

- Aborting a batch
- Adding a batch
- Putting a batch into AUTO mode
- Performing binding prompts
- Clearing all failures
- Holding a batch
- Putting a batch into Manual mode
- Performing operator prompts
- Removing a batch
- Restarting a batch

- Starting a batch
- Stopping a batch

#### **BatchAdd ActiveX Control**

- Adding a batch

#### **BatchOperatorPromptsList ActiveX Control**

- Acknowledging a prompt

#### **BatchBindingPromptsList ActiveX Control**

- Acknowledging a prompt

#### **BatchManualPhase ActiveX Control**

- Aborting a phase
- Acquiring a phase
- Clearing all failures
- Holding a phase
- Performing operator prompts
- Pausing a phase
- Releasing a phase
- Resetting a phase
- Restarting a phase
- Resuming a phase
- Starting a phase
- Toggling a phase's Step mode
- Stopping a phase

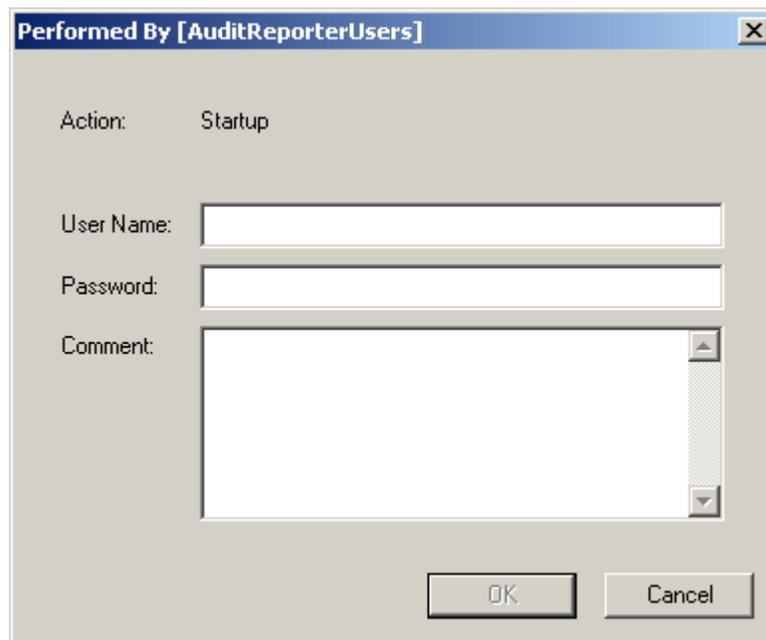
#### **BatchSFC ActiveX Control**

- Aborting a step
- Putting a step into Auto Mode
- Performing Binding Prompts
- Changing a step parameter
- Clearing all failures
- Holding a step
- Putting a batch into Manual Mode
- Performing operator prompts

- Restarting a step
- Starting a step
- Stopping a step
- Performing Transition Breakpoint Prompts

## Actions Available for Signing in the Audit Reporter

You can configure the Audit Reporter to require an electronic signature for opening the application and for extracting document data from a saved recipe or area model. After you enable electronic signatures in the Audit Reporter, you must enter a user name and password from the AuditReporterUsers Windows security group to start the Audit Report, as shown in the following figure.



*Electronic Signature Dialog Box in the Audit Reporter*

## Actions Available for Signing in the Batch Execution Configuration

You can configure electronic signatures to be required whenever you open the Batch Execution Configuration dialog box and/or whenever you save changes from it.

You can access the Batch Execution Configuration dialog box from the Batch Execution Workspace by double-clicking the Batch Execution Configuration in the WorkSpace tree. You can also double-click the Batch Execution Configuration in the Proficy iFIX WorkSpace tree to view this dialog box.

The following figure shows an example of a dialog box that requests a user name and password from a designated Windows security group before a save operation can be completed. Be aware that this example requests a user from the iESigAdministrators group for the Performed By signature, but this security group is configurable. It does not have to be the iESigAdministrators group.

**NOTE:** Batch Execution applies any changes you make in the Electronic Signature tab on a per node basis. All other tabs in the Batch Execution Configuration are applied on a per project basis.

The image shows a standard Windows-style dialog box titled "Performed By [iESigAdministrators]". The dialog contains the following elements:

- Action:** A label followed by the text "Save".
- User Name:** A text input field.
- Password:** A text input field.
- Comment:** A larger text area with a vertical scrollbar on the right side.
- Buttons:** "OK" and "Cancel" buttons located at the bottom right of the dialog.

*Electronic Signature Dialog Box in the Batch Execution Configuration*

---

## Tracking Electronic Signatures

Each time an operator signs for an action, a detailed electronic record is written to the electronic signature audit trail database. Batch Execution stores all electronic signatures generated by the Batch Execution Equipment Editor, Recipe Editor, WorkInstruction Editor, Audit Reporter, and configuration of electronic signatures in the Batch Execution WorkSpace.

Records written to the electronic signature audit trail:

- Ensure a tamper-resistant, time-stamped, permanent record of operator actions.
- Include the user names and full names of all operators and supervisors involved in signing and verifying actions.
- Include all comments entered by the operators and supervisors involved in signing and verifying actions.
- Include the name, version, and type of action from the application where the electronic signature was generated.
- Include the name, location, audit version number, and globally unique identifier (GUID) for the document.
- Include the computer name on which you ran the application and the logged in Windows user name.
- Include, in some instances, the area model or recipe file acted upon.

Refer to the Understanding Audit Versioning and the Audit Trail section for complete information about configuring audit trail messages for electronic signature and examples of signed messages sent to a relational database.

---

## Understanding 21 CFR Part 11

21 CFR Part 11 is a United States Government Food and Drug Administration (FDA)-mandated regulation that requires all electronic records and signatures, paperless records, and reporting procedures related to the manufacture of a product be captured and stored securely for businesses under its control, such as the Bio-Pharmaceutical and Food and Beverage industries. This regulation requires the protection, accuracy, and quick retrieval of all records. Secured, computer-generated, time-stamped audit trails must be available to independently record the date and time of operator actions that modify the manufacturing process.

Electronic records can be used to identify the ingredients and people involved in the production and distribution of regulated substances, such as prescription drugs. Electronic records also ensure accuracy, reliability, and security in data collection and record keeping.

Regulated industries that fail to meet 21 CFR Part 11 compliance risk the chance of Inspectional Observations (483s), warning letters, or the authorized shut-down of one or more operations.

The Electronic Signature option included with Batch Execution allows you to design an application that helps you to meet the demands of this regulation. The paperless environment that results from using this feature benefits you with faster information exchange, improved ability to integrate, trend, and search data, a reduction in errors, and reduced data storage costs.

### Using 21 CFR Part 11 Services from GE Intelligent Platforms

GE offers 21 CFR Part 11 consulting services to assist you with your goal of achieving 21 CFR Part 11 compliance. Using these services, you can reduce the time, effort, and expense of developing, implementing, and maintaining a compliant solution to meet the regulation. These services include:

- Training
- Assessment
- Detailed Detection
- Maintenance

For more information, refer to GE's web site <http://www.ge-ip.com>, or call your GE representative.

---

## Understanding Windows Security and Electronic Signatures

To configure security for electronic signatures, you can use existing Windows security groups and user accounts for Performed By and Verified By users, or define new Windows groups and user accounts.

---

## Using Local and Domain Groups

Batch Execution supports both local and domain groups in Windows. Upon receiving a request to validate a signature, Batch Execution checks the local computer for the specified group. If the group is not found, it then checks for a domain level group to verify the user name and password.

For example, you may choose to configure your Windows groups and user names on the Batch Execution Server computer or as part of your plant's overall domain security configuration.

---

## Example for Configuring Windows Security

You can create two groups, one named "Operator," and the other "Supervisor" to distinguish between personnel who can electronically sign a Performed By signature, and those who can sign a Verified By signature. The following section, Adding Operators and Supervisors, explains how to add operators and supervisors on the indicated operating systems within Windows security.

Although a user may belong to both the Performed By and Verified By security groups, Batch Execution does not allow that same user to enter both signatures. Batch Execution checks the user's full user name for comparison when determining if the same user is trying to sign for both the Performed By and Verified By signatures.

## Adding Operators and Supervisors

The following steps first describe how to add the user names of the operators and supervisors. The steps then outline how to add the actual Operator and Supervisor groups and assign users to each group.

### ►To add operators and supervisors:

1. Log in to Windows as an administrator, if you are not already.
2. Click the Start button, and point to Settings, Control Panel, Administrative Tools, and then Computer Management. The Component Services Microsoft® Management Console (MMC) snap-in appears.
3. In the System Tools folder, double-click the Local Users and Groups item.
4. Right-click the Users folder and select New User from the pop-up menu. The New User dialog box appears.
5. Enter information in the User Name, Full Name, Password, and Confirm Password fields.  
*NOTE: Batch Execution and WorkInstruction do not accept electronic signatures without a full user name defined.*
6. Click Create.
7. Repeat steps 5-6 for each individual user that you want to add.
8. Click Close.
9. Right-click the Groups folder and select New Group from the pop-up menu. The New Group dialog box appears.
10. Enter *Operator* in the Group Name field.

*NOTE: You do not have to use the group name Operator. You can use the group specific to your work flow. For example, you might enter PackingLineOperator instead of Operator.*

11. Click Add. The Select Users dialog box appears.
12. Enter a user name that you want to add to the Operator group, and then click OK.
13. Repeat steps 11-12 for each user you want to add to the Operator group.
14. After you finish adding users, click Create.
15. Repeat steps 9-14, but this time use Supervisor as the group name.

***NOTE:** You do not have to use the group name Supervisor. You can use the name of the supervisory group specific to your work flow. For example, you might enter ShiftManager instead of Supervisor.*

16. Click Close.

---

## Overview of Windows Security Groups

Although you create your own Operator and Supervisor groups for Performed By and Verified By users, Batch Execution also supplies some pre-defined Windows security groups for other electronic signature configuration functions. The sections that follow outline the user created and the Batch Execution created Windows security groups.

### User Created Windows Security Groups

The Windows security groups associated with electronic signatures that you create include:

**Operator** – Users from this security group (Performed By group) can sign for operator actions. This is just a suggested name; you can use another name for Performed By signatures if you prefer. If you use the WorkInstruction Demo, you must create this security group, however.

**Supervisor** – Users from this security group (Verified By group) can sign for supervisory actions. This is just a suggested name; you can use another name for Verified By signatures if you prefer. If you use the WorkInstruction Demo, you must create this security group, however.

### Batch Execution Created Windows Security Groups

The Windows security groups associated with electronic signatures that Batch Execution creates include the following:

**AuditReporterUsers** – Users from this security group are allowed to open the Audit Reporter application to generate, print, and export reports to XML, HTML, or Microsoft Excel formats. This group is created when you install the Batch Execution product. You can also retrieve an XML document associated with a Save or Save As action.

**iESigAdministrators** – Users from this security group can configure electronic signatures in the WorkInstruction Editor and Audit Reporter. This group is created when you install the Batch Execution product. The dialog boxes that request a user from this group to sign for configuration changes include the following:

- Database Login Configuration dialog box in the WorkInstruction Editor
- Electronic Signature tab of the Application Options dialog box in the Audit Reporter

Optionally, you can use this group for other authority checks, such as Performed By signatures that you may configure for opening or saving changes from the Batch Execution Configuration dialog box. The default signature settings for the Save command in the Batch Execution Configuration dialog box is Performed By, and the default security group is iESigAdministrators group. The security groups that you define for the Batch Execution Configuration changes are configurable; you do not have to use the iESigAdministrators security group for this purpose.

**iWorkUsers** – Users from this group can sign for Microsoft Visual SourceSafe actions, such as file check-ins and check-outs, in the WorkInstruction Editor. This group is created when you install the Batch Execution product. Refer to the WorkInstruction Manual for more information.

---

## Additional Considerations When Creating User Accounts

This section describes some considerations for Windows security when working in a 21 CFR Part 11 environment. It also overviews how to configure these features and how Windows security ties in with Batch Execution and WorkInstruction.

### Specifying the Full User Name

Although Windows security does not require you to define a full user name for user accounts, Batch Execution electronic signature validation requires that you specify a full user name for each user. If a user account does not have a full user name defined, the user is not validated, and the user cannot sign for any action in Batch Execution or WorkInstruction.

### Specifying the Number of Invalid Signature Attempts

Your system administrator defines the allowed number of failed signature attempts through Windows security. To perform this task in Windows security, you define the account lockout threshold for the user name. You must be logged in as an administrator to change this value. When a user surpasses the threshold value defined in Windows security, the account locks out and cannot be used again until the administrator resets it.

Since Batch Execution and WorkInstruction use Windows security settings for validating electronic signatures, if a user enters an incorrect password beyond the number of acceptable times defined in Windows security, Windows locks out the account for a configurable amount of time or until the administrator resets it.

For more information, refer to the account policy information in your Microsoft Windows system Help.

### Setting the Password Expiration for Users Performing Electronic Signatures

Your system administrator defines password expiration rules through Windows security. These rules include whether a user must change a password at the next logon, whether the password never expires, whether the account is disabled, or whether the user can change the password through Windows security. You must be logged in as an administrator to enable or change any of these settings. Since Batch Execution and WorkInstruction use security settings from Windows for validating electronic signatures, these products also use the same password expirations defined in Windows.

For more information, refer to the group and user account information in your Microsoft Windows system Help.

## **Tracking Invalid Signature Attempts with Windows Auditing**

You can track failed signature attempts in the same way your administrator tracks failed logon attempts on your Windows computers, since Batch Execution and WorkInstruction use Windows security. To do this, you define an audit policy to track failed login attempts. You must be logged in as an administrator to define or change an audit policy. To view the failed signatures, you view the security log in the Windows Event Viewer.

For more information, refer to the audit policy information and Event Viewer overview in your Microsoft Windows system Help.

## **Disallowing Blank Passwords**

Allowing for blank passwords for the users who sign electronic signatures is acceptable under Windows security; however, this is a security violation when working in a 21 CFR Part 11 environment. It is advised that you do not use blank passwords when creating your user accounts.

## **Disabling the Ability to Change the System Time**

You may want to disable an operator's ability to change the system time by removing the "Change the system time" user right from the appropriate user accounts in Windows security. By doing so, you can prevent inaccurate time stamps from entering the audit trail.

## **Other Considerations**

For other suggestions when defining local and domain security policies, and creating Windows groups and uses, refer to your Windows system Help.

---

# **Configuring Electronic Signatures**

You can configure actions to require one or two signatures, or none at all. If you configure one signature, Batch Execution requires a Performed By signature from the operator performing the command. If you configure two signatures, Batch Execution requires a Performed By signature from the operator and a Verified By signature from a supervisor to perform the command.

When Batch Execution requires two signatures (Performed By and Verified By), each signature must have a unique full user name defined in Windows security. This prevents a user with two accounts from signing for both signatures.

You configure electronic signatures for the Recipe Editor, Equipment Editor, and Batch Execution Configuration dialog box from the Batch Execution Workspace. You configure electronic signatures for the ActiveX controls from the associated Electronic Signature property page during design-time. You configure electronic signatures for the Audit Reporter within the Audit Reporter itself. The sections that follow describe each set of configuration steps in more detail. For information on configuring electronic signatures for WorkInstruction, refer to the WorkInstruction Manual.

---

## Overview for Configuring Electronic Signatures

To configure electronic signatures in your Batch Execution software, you must perform the tasks listed in the following steps.

### ►To configure electronic signatures:

1. Ensure that the computers used to configure and enter electronic signatures are equipped with hardware keys that have the electronic signature option enabled.
2. Define your Windows security groups and users for Operators and Supervisors. Refer to one of the following sections for more details:
  - Adding Operators and Supervisors
3. Configure the electronic signature option and associated Windows security group for actions in the Batch Execution software. Refer to the following sections for details on each component:
  - Configuring Electronic Signatures for the Recipe Editor, Equipment Editor, and the Batch Execution Configuration
  - Configuring Electronic Signatures for the ActiveX Controls
  - Configuring Electronic Signatures for the Audit Reporter

The sections that follow describe these configuration steps in more detail.

---

## License and Key Checking

To use the Electronic Signature option, you must purchase the option from GE and receive hardware keys with this functionality enabled. You will need to replace your current key or run an update program on your existing key to enable this option.

For older keys, use the GE iKeyDiag utility to view whether the electronic signature option is enabled on the computer you are working on.

For newer keys, use the Proficiency License Viewer to view whether the electronic signature option is enabled on the computer you are working on.

### ►To use iKeyDiag to determine if electronic signatures are enabled:

1. Click the Start button and then point to Run. The Run dialog box appears.
2. Type iKeyDiag in the Open field.
3. Click OK. The iKeyDiag utility appears.

*NOTE: You can also access the iKeyDiag utility from the iKeyDiag button on the Server tab in Batch Execution Server Manager.*

4. Click the Batch Execution tab.
5. Check if the Batch Execution Electronic Signature check box is selected.

If the Batch Execution Electronic Signature check box is selected, electronic signatures are enabled. If the feature is not enabled, this check box is cleared. For information on upgrading your key to include this option, contact GE. You will need to use the iKeyUpdate utility.

► **To use the Proficy License Viewer to determine if electronic signatures are enabled:**

1. From the Start menu, point to Programs, Proficy Common, and then License Viewer. The License Viewer appears.

***NOTE:** If you have a new key and you can't get the License Viewer to display, ensure that you ran the Microsoft .NET install program (dotnetfx.exe) after the Batch Execution product install. If you did not, you will need to install it in order to open the License Viewer. Refer to the "Viewing the Proficy License Viewer" section of the Release Notes tab in the Important Product Information (IPI) help for more information.*

2. In the Proficy Products list, scroll down and select the Batch Execution product. The License and Key Diagnostics area should now display the Batch Execution options.
3. Check that the Electronic Signatures option is enabled.

If Electronic Signatures are not listed as enabled, you will need to update your key. For information on upgrading your key to include this option, contact GE.

---

## **Configuring Electronic Signatures for the Recipe Editor, Equipment Editor, and the Batch Execution Configuration**

For the Batch Execution Recipe and Equipment Editors, you configure electronic signatures for commands on a per node basis. Additionally, when you configure your Batch Execution system, you can define electronic signatures to be required whenever a user opens and/or saves changes for any tab of the Batch Execution Configuration dialog box.

To configure any electronic signatures for these applications, you must select the Enable Batch Execution Auditing check box in the Electronic Signature tab in the Batch Execution Configuration dialog box.

After you enable this option, a user must enter his user name and password from the Windows security groups specified in the Performed By and Verified By fields specified for each command (unless you specified None as the signature type). Batch Execution records the computer name or logged in user name in the database when performing a command, regardless of the signature type.

► **To configure electronic signatures for a node:**

1. Open the Proficy Batch Execution WorkSpace.
2. Open the Configuration folder in the Batch Execution WorkSpace tree.
3. Double-click the Batch Execution Configuration item in the WorkSpace tree. The Batch Execution Configuration dialog box appears.
4. Select the Electronic Signature tab in the Batch Execution Configuration dialog box.

***NOTE:** Batch Execution applies any changes you make in the Electronic Signature tab on a per node basis. All other tabs in the Batch Execution Configuration are applied on a per project basis.*

5. Select the Enable Batch Execution Auditing check box.
6. Enter a data source name (DSN) for the electronic signature auditing database, and a user name and password for that database.
7. Select the signature requirements for the Batch Execution Configuration dialog box.
8. Select the signature requirements for the Recipe Editor.
9. Select the signature requirements for the Equipment Editor.

**NOTE:** If you want to assign the same requirements to each action, use the Default drop-down field for the specified editor. Otherwise, select a signature type from the drop-down list for each command. Right-click the Performed By or Verified By field to browse the Windows Security Groups.

The following figure shows an example of signature requirements defined for the Batch Execution Configuration, Recipe Editor, and Equipment Editor.

The figure displays three dialog boxes, each with a table of signature requirements. The first dialog, 'Batch Execution Configuration', has a checkbox for 'Use Default Signature Requirements' which is unchecked. Its table lists 'Default', 'Launch', and 'Save' commands. The second dialog, 'Recipe Editor', has a checked checkbox for 'Use Default Signature Requirements'. Its table lists 'Default', 'Convert Project Storage', 'New', 'Open', 'Print', 'Rebuild Recipe Directory', and 'Release To Production' commands. The third dialog, 'Equipment Editor', has an unchecked checkbox for 'Use Default Signature Requirements'. Its table lists 'Default', 'Export', 'Import', 'New', 'Open', 'Print', and 'Save' commands.

Batch Execution Configuration			
<input type="checkbox"/> Use Default Signature Requirements			
Command	Signature Requirements	Performed By	Verified By
Default	None		
Launch	Performed By	iESigAdministrators	
Save	Performed By	iESigAdministrators	

Recipe Editor			
<input checked="" type="checkbox"/> Use Default Signature Requirements			
Command	Signature Requirements	Performed By	Verified By
<b>Default</b>	<b>Performed By/Verified By</b>	<b>Operator</b>	<b>Supervisor</b>
Convert Project Storage	None		
New	None		
Open	None		
Print	None		
Rebuild Recipe Directory	None		
Release To Production	None		

Equipment Editor			
<input type="checkbox"/> Use Default Signature Requirements			
Command	Signature Requirements	Performed By	Verified By
Default	None		
Export	Performed By	Operator	
Import	Performed By	Operator	
New	None		
Open	None		
Print	None		
Save	Performed By/Verified By	Operator	Supervisor

Example of Signature Requirements in Electronic Signature Tab

In this example, in order to open or save any changes to the Batch Execution Configuration dialog box, a Performed By user name and password from iESigAdministrators group is required. The Recipe Editor requires a default signature type with the Performed By signature from a user in the Operator security group and a Verified By signature from a user in the

Supervisor group, for all actions. The Equipment Editor has different signature requirements for each command.

10. Click OK. The Performed By dialog box appears.

11. Enter an electronic signature from the iESigAdministrators dialog box and click OK.

***NOTE:** If you want to configure other Batch Execution nodes with the same audit configuration, copy the Auditcfg.ini file from the folder of the local computer to the same folder for each node you want to configure. For Windows Vista or Windows Server 2008, the file is located in the C:\ProgramData\Proficy\Proficy Batch Execution\Configs folder. For Windows XP or Windows Server 2003, the file is located in the C:\Documents and Settings\All Users\Application Data\Proficy\Proficy Batch Execution\Configs folder.*

## Understanding iFIX Security and Batch Execution Electronic Signatures

iFIX security checking *does not* occur on commands that you configured an electronic signature for (either a Performed By or a Performed By/Verified By signature) in the Batch Execution Equipment or Recipe Editors. To configure electronic signatures, you must first enable auditing and assign a signature requirement as a default, or on a per command basis, as described in the Configuring Electronic Signatures for the Recipe Editor, Equipment Editor, and the Batch Execution Configuration section.

If you do not use electronic signatures, iFIX security checking *does* occur for specific commands in the Batch Execution Equipment and Recipe Editors. You can have auditing enabled, without electronic signatures, and iFIX security checked. In this case, you select the Enable Batch Execution Auditing check box in the Electronic Signature tab in the Batch Execution Configuration dialog box, but select None as the signature requirement for all commands. A list of the commands for which iFIX security checking can occur are outlined in the following sections.

### The Batch Execution Equipment Editor and iFIX Security Checking

iFIX security checking can occur for the following commands in the Batch Execution Equipment Editor, if electronic signatures are not required:

- Startup
- New
- Save
- Save As

All other commands in the Batch Execution Equipment Editor do not check iFIX security.

### The Batch Execution Recipe Editor and iFIX Security Checking

iFIX security checking can occur for the following commands in the Batch Execution Recipe Editor, if electronic signatures are not required:

- Startup
- New
- Save

- Save As
- Remove
- Rebuild Recipe Directory
- Release To Production

All other commands in the Batch Execution Recipe Editor do not check iFIX security.

---

## Configuring Electronic Signatures for the ActiveX Controls

The ActiveX controls provide property pages that designers or operators can use to view and change the controls' properties. You can only edit the Electronic Signature property page at design-time only.

After you enable the electronic signature option, a user must enter his user name and password from the Windows security groups specified in the Performed By and Verified By fields for each command at run-time (unless you selected None as the signature type).

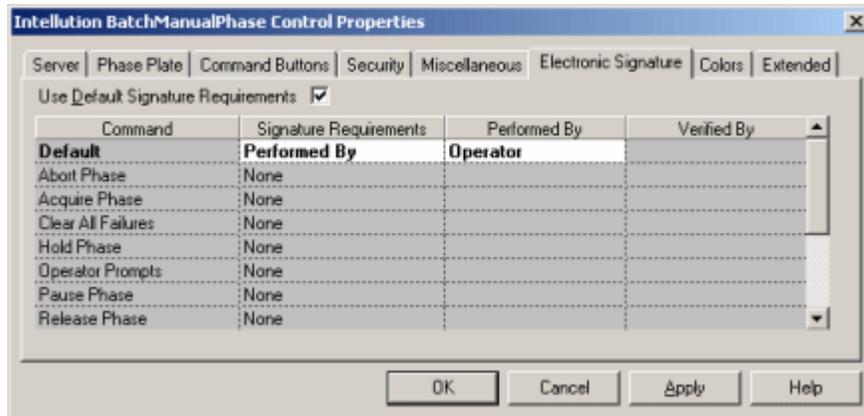
### ►To configure electronic signatures in a Batch Execution ActiveX control:

1. Open the control in any design-time OLE container.
2. Right-click the control and select Properties from the pop-up menu. The control's property pages appear.
3. Select the Electronic Signature property page.
4. Select the Use Default Signature Requirements check box if you want to use a default signature.
5. Select the signature type for the default, or for each command listed (if default is not selected):
  - Performed By
  - Performed By / Verified By
  - None
6. Select the Windows security group for each Performed By and Verified By signature specified.

***NOTE:** Right-click on the edit box and select the Browse option to open the Windows Security Groups dialog box. Make sure that the cursor is not displaying in the text box when you right-click on it. Select a group from the Windows Security Groups dialog box and click OK. You can only browse local security groups, but you can manually enter a domain group.*

7. Click OK to save your changes.

As shown in the following figure, the Electronic Signature property page is similar to the Electronic Signature tab in the Batch Execution Configuration dialog box in the WorkSpace.



*Example of Electronic Signature Property Page in the Batch Execution ActiveX Controls*

The previous figure shows how you would configure a default signature for all commands in ActiveX control as the Performed By signature type, and requires a user from the Operator group to sign the Performed By electronic signature.

---

## Configuring Electronic Signatures for the Audit Reporter

You configure electronic signatures for the Audit Reporter, within the Audit Reporter itself. You must be a member of the iESigAdministrators Windows security group to configure electronic signatures in the Audit Reporter. Because the Audit Reporter requires the user to be a member of a separate Windows security group to enable the electronic signature feature, not all users can enable or disable electronic signatures in the Audit Reporter.

To enable or disable the electronic signature feature, the user must be a member of the iESigAdministrators security group, or he cannot disable or enable electronic signatures in the Audit Reporter. This provides an additional level of security for electronic signatures.

After you enable the electronic signature feature, a user must enter his user name and password from the AuditReporterUsers Windows security group whenever the user starts the Audit Report, or extracts the document associated with the save action from the Batch Execution Recipe or Equipment Editor.

### ►To configure the electronic signature feature in the Audit Reporter:

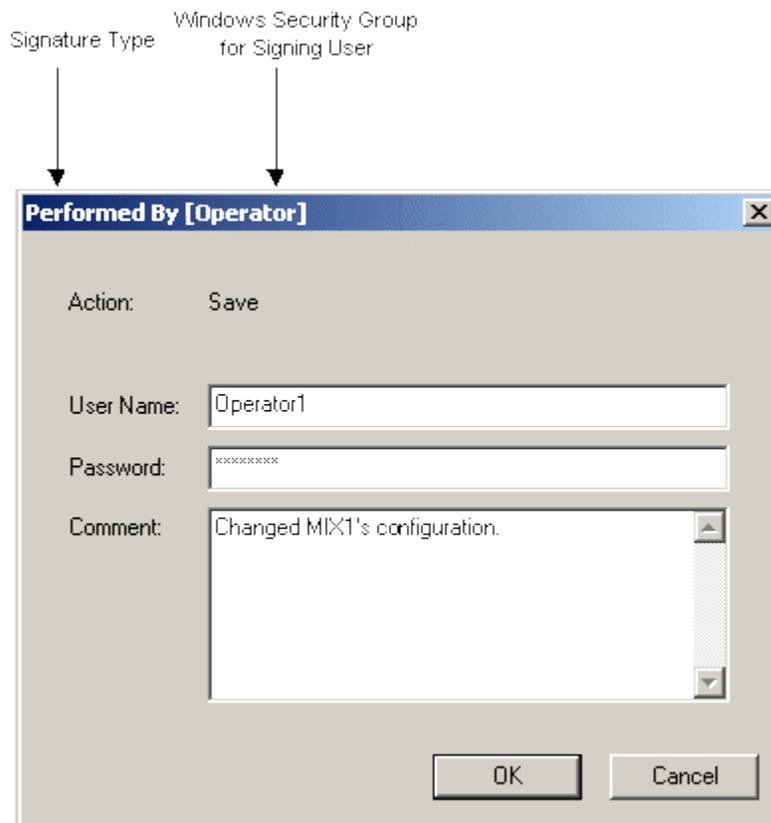
1. Start the Audit Reporter.
2. On the Tools menu, click Options > Electronic Signature. The Electronic Signature dialog box appears.
3. Select the Enable Authority Check check box.
4. Click OK. A prompt appears requesting an electronic signature.
5. Enter an electronic signature from the iESigAdministrators security group.

## Performing Electronic Signatures

When an action requires an electronic signature, a dialog box appears, requesting a user name and password. The first dialog box that appears requests a signature from an operator from the Performed By group. If a second dialog box appears, it requests a signature from a supervisor from the Verified By supervisor group. The signature type and group name from which the user must belong to, in order to sign for the command, is listed in the title bar of the dialog box. You can optionally enter a comment with the signature.

### Example of Electronic Signature Dialog Box

In the following figure, Batch Execution requests a Performed By signature type. The group from which the user must belong to is the Operator group. The user name entered is Operator1; Operator1 must be a member of the Operator group for the signature to be validated and the action to proceed. An optional comment is entered in the comment field.



Performed By Electronic Signature Dialog Box

**NOTE:** The Operator1 user name is a generic example; the user names that you use in your Windows security setup be more specific to an operator's actual name or function.

## What Happens if the Signature Fails?

If a signature fails, Batch Execution does not perform the command, nor is the event logged to the Batch Execution system tables. A message box appears with an error message. To track these failed attempts, you need to configure an audit policy in your Windows security to do so.

---

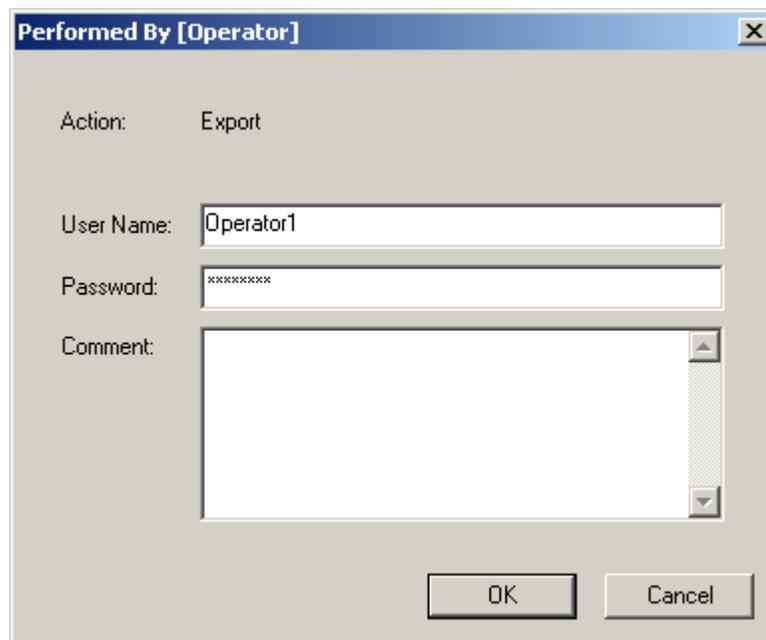
## Examples of Electronic Signatures

The following examples illustrate the indicated Electronic Signature feature in the Batch Execution product:

- Performed By Signature
- Performed By/Verified By Signature
- Comments with an Electronic Signature
- Performed By Signature in the ActiveX Controls
- Performed By/Verified By Signature in the ActiveX Controls

### Performed By Signature

The following figure displays an example of a Performed By signature. This Electronic Signature dialog box requests a user name and password from the Operator group to perform an Export action in the Equipment Editor.



The image shows a Windows-style dialog box titled "Performed By [Operator]". The dialog box has a light gray background and a blue title bar. It contains the following elements:

- Action:** A label followed by the text "Export".
- User Name:** A text input field containing the text "Operator1".
- Password:** A text input field containing seven asterisks "\*\*\*\*\*".
- Comment:** A large, empty text area with a vertical scrollbar on the right side.
- Buttons:** Two buttons at the bottom right, labeled "OK" and "Cancel".

## Performed By/Verified By Signature

The following figure displays an example of a Performed By/Verified By signature. In this example, the Performed By signature was already signed by a user with a full name of "Jim Sheridan" and verified by Batch Execution, so the Performed By fields are unavailable. A time stamp displays the date and time when Batch Execution authenticated the electronic signature of the operator (in the Performed By group). A user name and password from the Supervisor group is requested to complete the Export action in the Equipment Editor.

The image shows a dialog box titled "Verified By [Supervisor]". Inside the dialog, there is a section with the following information:

- Action: Export
- Performed By: Jim Sheridan
- Timestamp: July 01 2002 12:25:38

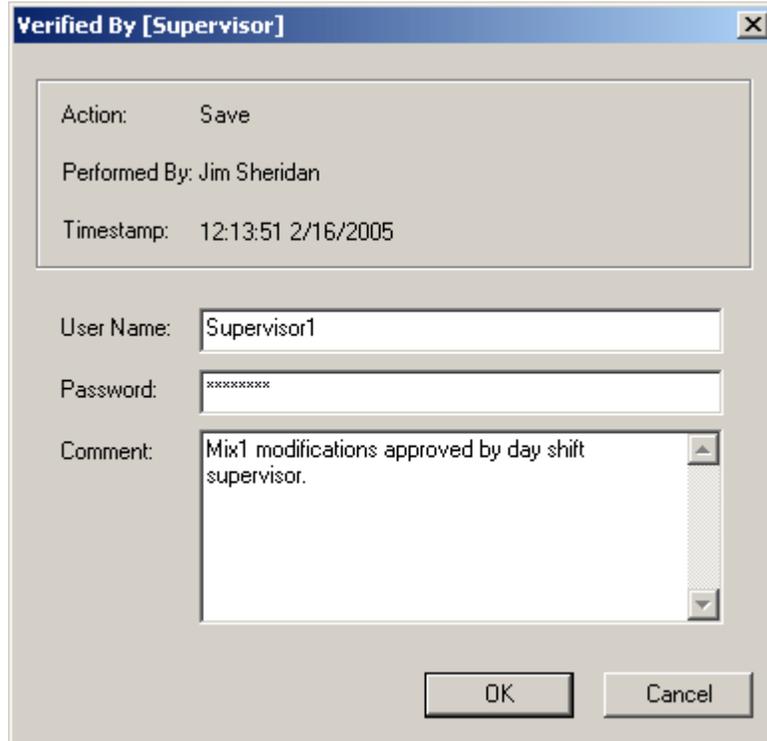
Below this information, there are three input fields:

- User Name: Supervisor1
- Password: \*\*\*\*\*
- Comment: (An empty text area with a vertical scrollbar on the right side.)

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

## Comments with an Electronic Signature

The following figure displays an example of user comments included with a Verified By signature. The Performed By signature was already signed by a user with a full name of "Jim Sheridan" and verified by Batch Execution, so the Performed By fields are unavailable. The Electronic Signature dialog box requests a user name and password from the Supervisor group to complete the Save action. The optional comment is entered below the User Name and Password fields for the Verified By signature.



*NOTE: The Performed By signature can not be the same as the Verified By signature.*

## Performed By Signature in the ActiveX Controls

Unlike the Performed By signature that appears in other Batch Execution applications, the Performed By signature for the ActiveX controls does not include a field for optional comments. The following figure displays an example of a Performed By signature from the BatchList ActiveX control. This Electronic Signature dialog box requests a user name and password from the Operator group in order to put the batch into Manual mode.



## Performed By/Verified By Signature in the ActiveX Controls

Unlike the Performed By/Verified By signature that appears in other Batch Execution applications, the Performed By/Verified By signature for the ActiveX controls does not include a field for optional comments. In the following example, the Performed By signature was already signed by a user with a full name of "Jim Sheridan" and validated by Batch Execution, so the Performed By fields are unavailable. To complete the signing, a Verified By signature is required to create the batch in the BatchAdd control.

The BatchAdd control actually embeds the electronic signature request into the last page of the Create Batch wizard, as shown in the following figure. This screen includes a Validate button instead of an OK button to validate the Performed By electronic signature. In the example, this button is unavailable since Batch Execution already validated the signature. You click the Finish button to validate the Verified By signature. You can only access this screen from the Create Batch wizard if an electronic signature is required.

The screenshot shows a Windows-style dialog box titled "Create Batch Wizard 4 of 4". It contains two main sections for user information. The first section, "Performed By [Operator]", includes a "User Name" field with "Operator1", a "Password" field with masked characters, a "Timestamp" field with "15:09:50 2/16/2005", and a "Validate" button. The second section, "Verified By [Supervisor]", includes a "User Name" field with "Supervisor1", a "Password" field with masked characters, and an empty "Timestamp" field. At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

---

## Examples of Failed Signing Attempts

If a signature fails, Batch Execution does not perform the command, nor is the event logged to the Batch Execution system tables. A message box appears with an error message. This section displays some of the common error messages that your users may encounter.

### Invalid User Name or Password

When signing an electronic signature, if a user enters a user name that does not exist in the requested group or uses an invalid password, the following message box appears. If you accidentally misspell the user name or password, click OK for the message, and enter the user name and password again. The Electronic Signature dialog box does not leave the screen until you click Cancel.



## Account Expired

When signing an electronic signature, if a user enters a user name and password from an expired account, the following message box appears. You will not be able to sign for an action in Batch Execution until your Windows Administrator enables the account again.



## User Not a Member of the Required Group

When signing an electronic signature, if a user enters a valid user name and password but the user account is not a member of the group required for signing, the following message box appears. You can only sign for the action if the user is a member of the group displayed in the title bar of the Electronic Signature dialog box.



## The Same Full User Name Not Accepted for Both Signatures

When signing an electronic signature, if the user names are different, but the full user names are the same for both the Performed By and Verified By signatures, Batch Execution does not perform the command. The following message box appears after the second signature is entered. Enter another user, with a different full user name, in the Verified By dialog box if you want the command to proceed.



### The Same User Cannot Sign Both Signatures

When signing an electronic signature, if the user names are the same for both the Performed By and Verified By signatures, Batch Execution does not perform the command. The following message box appears after the second signature is entered. Enter another user name in the Verified By dialog box if you want the command to proceed.



### Electronic Signature Request Cancelled from the Audit Reporter

If a user cancels the electronic signature request when opening the Audit Reporter the following message box appears. You can only open the Audit Reporter if you enter a valid user name and password from the AuditReporterUsers security group.



### Security Group Does Not Exist on the Domain

If the security group to which the user belongs to does not exist on your current domain, the following message box appears. Check that you are logged into the correct domain, and that you did not mistype the name of the Windows security groups when configuring the electronic signature options.



---

# Understanding Audit Versioning and the Audit Trail

Batch Execution and WorkInstruction provide an audit trail that contains a time-stamped data trail of actions performed within the Batch Execution and WorkInstruction applications. Each time an operator performs an action, with or without an electronic signature, a detailed electronic record is written to the audit trail database.

You can track both design-time and run-time audit information. For instance, you can track design-time audit information for developers using the WorkInstruction and Batch Execution Editors. Batch Execution records run-time audit information, when you schedule a batch, that tracks the version of the recipe executed by the batch.

Batch Execution includes an Audit Reporter application to view design-time audit information. You can also extract the data in the audit tables via third party software.

The sections that follow provide an overview of how all aspects of auditing work and explains how to configure and view the audit information in the Batch Execution applications.

---

## Automatic Versioning of Area Models and Recipes

Batch Execution implements automatic versioning of the recipe and area model files. When you create a recipe or area model, Batch Execution assigns a globally unique identifier (GUID) to it. Each time you create a file or use the Save As command to create a new file, Batch Execution generates a GUID for the file. The GUID distinguishes the file from older instances of the same file name in your audit database table.

For example, if you have a recipe file named Mix10.UOP with a GUID of 8D615AA0516511D69B7800C04F256E1A, the audit history and GUID for this file exist in your audit database table. If you delete the Mix10.UOP recipe file, and then later create a new recipe file with the same name, Batch Execution assigns a different GUID to the file to make this new instance of the recipe unique from the older instance. The GUID allows you to distinguish the two different instances of the recipe file in the database.

When Batch Execution first assigns the GUID, it assigns an audit version number of 1. Each time you save the file with changes, the audit version automatically increments by one. However, for recipe files that include sub-recipes, the audit version number of the sub-recipe file does not increment unless there is a change in the sub-recipe itself or in the area model.

When you save a file, Batch Execution streams the contents of the file out as an XML document to the audit trail in the database. The GUID for the file does not change, unless you use the Save As command.

An example of the audit information captured with the area model in the Equipment Editor is shown in the following figure.



Example of the Audit Information Dialog Box

## What is Captured with the Audited Document?

The audited information for the recipe or area model can be displayed in the Audit Information dialog box. The following table outlines the fields displayed in the Audit Information dialog box.

Fields in the Audit Information Dialog Box	
Field	Description
Audit Version	<p>Displays the audit version number of the currently configured area model or recipe file.</p> <p>The audit version number increases by one each time you save the area model or recipe.</p> <p><b>NOTE:</b> For recipe files that include sub-recipes, the audit version number of the sub-recipe file does not increment unless there is a change in the sub-recipe itself or in the area model.</p>
Unique Identifier	<p>Displays the unique, system-generated identifier for the area model or recipe.</p> <p>Batch Execution generates the GUID when you save a new area model or recipe for the first time, or use the Save As command to save the area model or recipe.</p>

<b>Fields in the Audit Information Dialog Box</b>	
<b>Field</b>	<b>Description</b>
Performed By Group Box	Information only appears in the fields of this group box if you enabled auditing and configured Save or Save As signature requirements in the Batch Execution Configuration dialog box in the Batch Execution WorkSpace, and then saved the area model with the required electronic signatures.
User Name	Displays the Windows user name of the operator (from the Performed By group) who last authorized the saving of the area model or recipe.
Full Name	Displays the Windows full user name of the operator (from the Performed By group) who last authorized the saving of the area model or recipe.
Timestamp	Displays the date and time when Batch Execution authenticated the electronic signature of the operator (from the Performed By group).
Comment	Displays any comments entered by the operator (from the Performed By group) who last authorized the saving of the area model or recipe. The maximum length of this field is 1024 characters.
Verified By Group Box	Information only appears in the fields of this group box if you enabled auditing and configured Save or Save As signature requirements in the Batch Execution Configuration dialog box in the Batch Execution WorkSpace, and then saved the area model with the required electronic signatures (and the signature included a Verified By signature).
User Name	Displays the Windows user name of the supervisor (from the Verified By group) who last authorized the saving of the area model or recipe.
Full Name	Displays the Windows full user name of the supervisor (from the Verified By group) who last authorized the saving of the area model or recipe.
Timestamp	Displays the date and time when Batch Execution authenticated the electronic signature of the supervisor (from the Verified By group).
Comment	Displays any comments entered by the supervisor (from the Verified By group) who last authorized the saving of the area model or recipe. The maximum length of this field is 1024 characters.

## Viewing the Design-time Audit Information

You can view audit information for a document from the following Batch Execution applications:

- Batch Execution Recipe Editor
- Batch Execution Equipment Editor
- Batch Execution WorkSpace
- Batch Execution Audit Reporter
- Batch Execution Server Manager

The following sections explain how to access audit information from each of these indicated Batch Execution applications.

### ▶To view audit information for a file in the Recipe Editor:

On the Recipe menu, click Audit Information. The Audit Information dialog box appears with the audit versioning information for that file. You can also right-click in the design area of the Recipe Editor and select the Audit Information option from the right-click menu to display this dialog box.

### ▶To view audit information for a file in the Equipment Editor:

On the File menu, click Audit Information. The Audit Information dialog box appears with the audit versioning information for that file.

### ▶To view audit information in the Batch Execution WorkSpace:

On the Area menu, click Audit Information. The Audit Information dialog box appears with the audit versioning information for that file.

### ▶To view audit information for a file in the Audit Reporter:

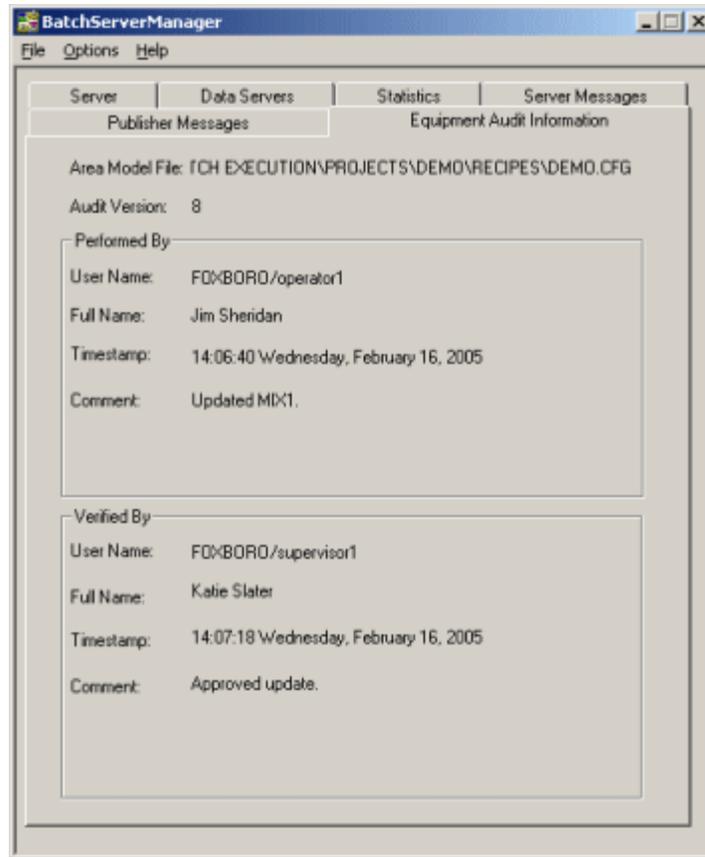
Run a report in the Audit Reporter to view the audit information for a file. The audit trail appears for all files. To view the audit information for a specific file, locate it in the spreadsheet output. If the file does not display in the report, change the report template parameters, as described in the Audit Reporter Help.

### ▶To view audit information for a project from the Batch Execution Server Manager:

Select the Equipment Audit Information tab in the Batch Execution Server Manager. The Audit Information dialog box appears with the audit versioning information for that file. If you re-save an area model and the Batch Execution Server is running, you must stop and restart the Batch Execution Server to display the newly audited file information in the Equipment Audit Information tab. This is the same procedure that you use to reload a new project in the Batch Execution Server Manager.

## Example of Viewing Design-time Audit Information

The following figure shows an example of the audit information displayed in the Batch Execution Server Manager.



*Example of Audit Information Displayed in the Batch Execution Server Manager*

---

## Using the Audit Reporter to View the Audit Trail

With the Audit Reporter, you can view the design-time audit trail data for your Batch Execution system. This data includes the commands developers performed, with the required electronic signatures, from these Batch Execution applications: the Recipe Editor, Equipment Editor, Batch Execution Configuration in the WorkSpace, the WorkInstruction Editor, and the Audit Reporter.

Through the Audit Reporter, you can quickly generate a report to examine the change history of the files (also called documents) saved in these applications. After generating the report, plant personnel may print or export reports to XML, HTML, or Microsoft® Excel® formats.

The Audit Reporter also allows you to save report criteria, in the form of templates, for reports that you run repeatedly. The Audit Reporter stores these templates in the database. For instance, in a report template you can predefine searches that you want to perform on the database, and include specific headers and footers for the reports, if you want to print them. You can then run a report again without having to redefine the formatting each time.

All three Batch Execution Editors include toolbar buttons to launch the Audit Reporter with a single click. The following figure shows a sample report in the Audit Reporter.

	Application	Action	Action Timestamp	Performer UserID	Performer Full Name	Performer Signature	Performer Security
1	Batch Execution Electronic Signature	Save	1/13/2005 9:54:07 AM	NGRW000\oper7	Gay H. Scott	1/13/2005 9:54:07 AM	ESigAdministrators
2	Batch Execution Equipment Editor	Open	1/13/2005 9:54:31 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 9:54:42 AM	Operators
3	Batch Execution Equipment Editor	Open	1/13/2005 9:55:29 AM	BOSTON\oper8	Kelly Ann Bolger	1/13/2005 9:55:45 AM	Operators
4	Batch Execution Recipe Editor	Startup	1/13/2005 9:56:15 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 9:56:10 AM	Operators
5	Batch Execution Recipe Editor	Convert	1/13/2005 9:56:50 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 9:56:30 AM	Operators
6	Batch Execution Recipe Editor	Save	1/13/2005 9:56:50 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 9:56:41 AM	Operators
7	Batch Execution Recipe Editor	Startup	1/13/2005 9:58:31 AM	BOSTON\oper8	Kelly Ann Bolger	1/13/2005 9:58:11 AM	Operators
8	Batch Execution Recipe Editor	Open	1/13/2005 9:58:44 AM	BOSTON\oper8	Kelly Ann Bolger	1/13/2005 9:58:39 AM	Operators
9	Batch Execution Recipe Editor	Convert	1/13/2005 10:00:08 AM	BOSTON\oper8	Kelly Ann Bolger	1/13/2005 9:59:41 AM	Operators
10	Batch Execution Recipe Editor	Save	1/13/2005 10:00:09 AM	BOSTON\oper8	Kelly Ann Bolger	1/13/2005 9:59:57 AM	Operators
11	Batch Execution Equipment Editor	Open	1/13/2005 10:15:10 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 10:15:17 AM	Operators
12	Batch Execution Equipment Editor	Open	1/13/2005 10:16:41 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 10:16:48 AM	Operators
13	Batch Execution Recipe Editor	Startup	1/13/2005 10:18:39 AM	HINGHAM\super1	Daniel H. McKenna	1/13/2005 10:18:15 AM	Supervisors
14	Batch Execution Recipe Editor	Open	1/13/2005 10:18:52 AM	HINGHAM\super1	Daniel H. McKenna	1/13/2005 10:18:47 AM	Supervisors
15	Batch Execution Recipe Editor	Save	1/13/2005 10:19:17 AM	HINGHAM\super1	Daniel H. McKenna	1/13/2005 10:19:11 AM	Supervisors
16	Batch Execution Recipe Editor	Verify	1/13/2005 10:19:31 AM	BOSTON\oper8	Kelly Ann Bolger	1/13/2005 10:19:26 AM	Operators
17	Batch Execution Recipe Editor	Verify	1/13/2005 10:19:31 AM	HINGHAM\super1	Daniel H. McKenna	1/13/2005 10:19:26 AM	Supervisors
18	Batch Execution Recipe Editor	Verify	1/13/2005 10:19:32 AM	FOXBOARD\oper1	Dan Smith	1/13/2005 10:19:26 AM	Operators
19	Batch Execution Recipe Editor	Save	1/13/2005 10:19:32 AM	HINGHAM\super1	Daniel H. McKenna	1/13/2005 10:19:11 AM	Supervisors

*Audit Reporter Application - Sample Report*

Refer to the Audit Reporter application Help for information on how to run a report.

## What Types of Data Does the Audit Trail Store?

Each record in the audit trail contains the following information:

- Name of the application from which the electronic signature was generated.
- Version of the application.
- Command invoked by the operator.
- Timestamp when the command was invoked.
- Signature type: one (Performed By), two signatures (Performed By/Verified By), or no signatures.
- Signature information (user name, user full name, Windows security group, time stamp, and comment, if entered).
- Name for the document.
- Audit version number for the document.
- Globally unique identifier (GUID) for the document.
- Computer name that the application resided on and the Windows user name logged into that computer.
- Logged in iFIX user name.
- XML representation of the document (when you invoke either the Save or Save As command).

For more detailed information on the audit trail table, see the AUDITTABLE Table section.

---

## Viewing Audited XML Documents

Each time you save the area model or recipe file (current level only) with changes, Batch Execution streams the contents of the file out as an XML document to the audit trail in the database. This record of the audited document file is saved in the database as a Binary Large Object (BLOB) data type. Use the Audit Reporter application to view the XML version of the audited file.

### ►To view the audited XML file:

1. Open the Batch Execution Audit Reporter.
2. Make sure that you include the AuditDocumentData column in your report output:
  - a. Select Template from the Report menu to open the Report Template dialog box.
  - b. Click the Columns tab and scroll to the end of the list.
  - c. Make sure you selected the check box that appears next to the AuditDocumentData column.

3. Run a report.

4. Select the row from which you want to obtain an XML version of the audited document.

*NOTE: You can only obtain an XML version of the document for rows that are the result of a Save or Save As action in the Recipe, Equipment Editor, or WorkSpace. The Audit Reporter displays paper clips in the Document Data field of these rows.*

5. Select Retrieve Document from the Report menu. The Retrieve Document dialog box appears.

*NOTE: You can also double-click the AuditDocumentData field to display the Retrieve Document dialog box.*

6. Enter the name that you want to save the XML document as in the File Name field.

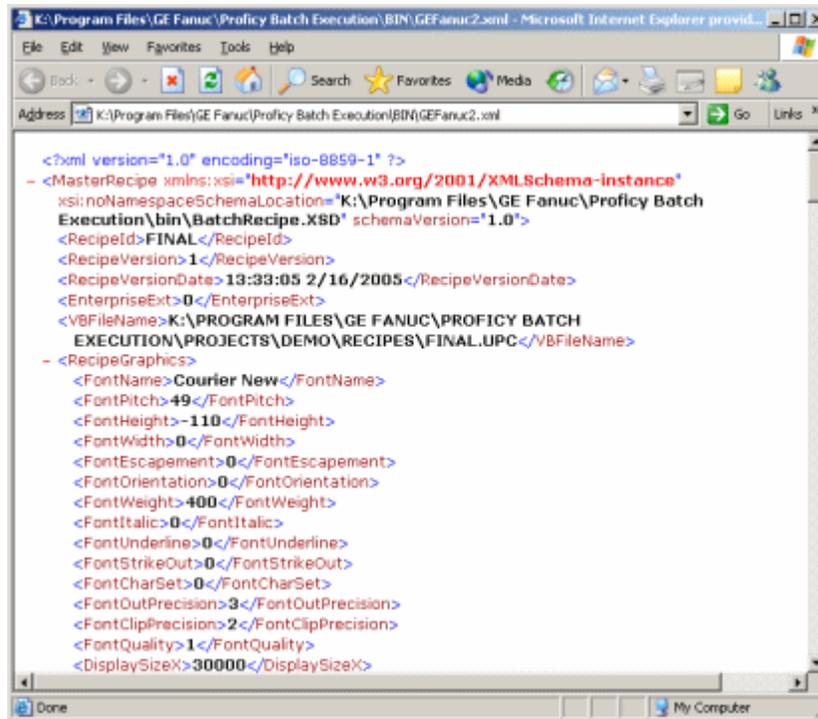
7. Select a location to save the file to.

8. Click OK.

9. Browse to the folder that you saved the file to in Windows Explorer to view the XML document.

## Example of an XML Schema

You can view an XML document through Microsoft® Internet Explorer®, a text editor, or any XML editor. The following figure displays an example of an XML document for an audited version of a master recipe. This output is displayed in Microsoft Internet Explorer.



Example of an XML Document Representing an Audited Recipe

You can also view the XML file by writing your own code to export the AuditDocumentData field from the AUDITTABLE database. The Audit Reporter, however, provides a quick way to extract the audited version of the document.

---

## Enabling Auditing

You can audit user actions in the following Batch Execution applications:

- Batch Execution Configuration dialog box
- Recipe Editor
- Equipment Editor
- Audit Reporter
- WorkInstruction Editor

You can quickly view the audit trail from the Audit Reporter. The actions that you can audit against are described in the What Determines a Signed Action? section.

For more information on configuring auditing in the WorkInstruction Editor, refer to the WorkInstruction Manual. In the WorkInstruction Editor, you can audit all Document Management System (DMS) actions, including all document check-in and check-out actions.

For information on the information captured by the ActiveX controls, refer to the BATCH\_CMD\_SIGNATURE\_SUCCESS Table section.

## Configuring Auditing in the Batch Execution Recipe and Equipment Editors

In the Batch Execution Recipe and Equipment Editors, you configure auditing for commands on a per node basis.

### ►To configure auditing for a node:

1. Open the Proficy Batch Execution WorkSpace.
2. Open the Configuration folder in the Batch Execution WorkSpace tree.
3. Double-click the Batch Execution Configuration item in the WorkSpace tree. The Batch Execution Configuration dialog box appears.
4. Select the Electronic Signature tab in the Batch Execution Configuration dialog box.
5. Select the Enable Batch Execution Auditing check box.
6. Enter a data source name (DSN) for the electronic signature auditing database, and a user name and password for that database.
7. Configure the signature requirements for the commands in the Batch Execution Recipe and Equipment Editors, or leave them set to None.
8. Click OK.

## Configuring Auditing in the Audit Reporter

You configure auditing for the Audit Reporter directly within the Audit Reporter. You must be a member of the iESigAdministrators Windows security group to configure electronic signatures in the Audit Reporter.

After you enable the auditing feature, a user must enter a user name and password from the AuditReporterUsers Windows security group whenever the user starts the Audit Report, or extracts document data from a saved recipe or area model. Unlike the Recipe and Equipment Editors, if you enable auditing in the Audit Reporter, you also enable electronic signatures. You cannot set the electronic signature requirement to None in the Audit Reporter.

### ►To configure the audit trail in the Audit Reporter:

1. Start the Audit Reporter.
2. On the Tools menu, click Options. The Application Options dialog box appears.
3. Select the Electronic Signature tab.
4. Select the Enable Authority Check check box.
5. Click OK.

## Using Auditing Without Capturing Signatures

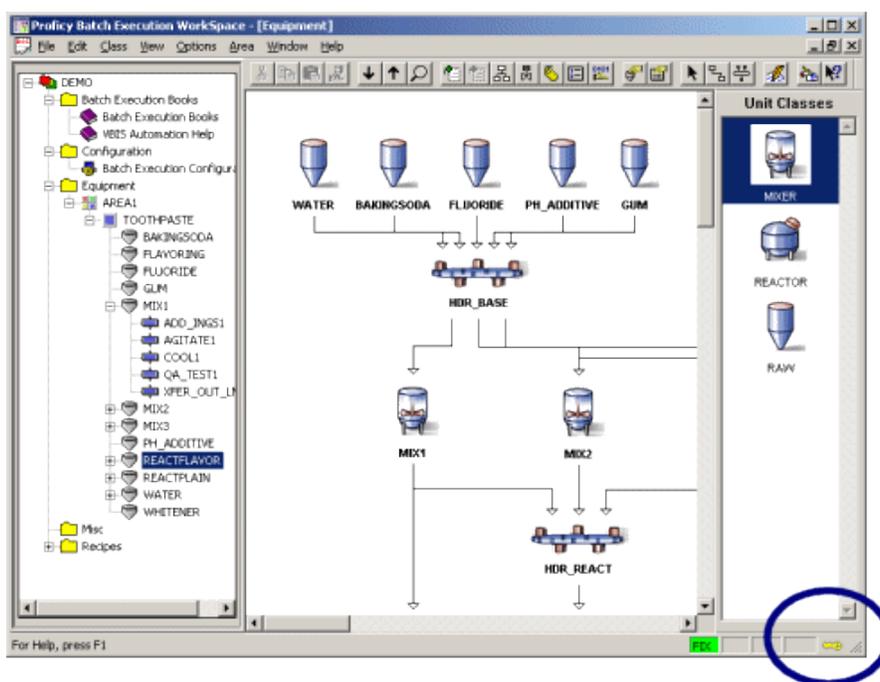
For auditing, Batch Execution can track the computer name or login user name when a command is performed, instead of an electronic signature. This allows you to capture the time-stamped actions that users performed on your computer, without capturing electronic signatures.

You can only use this auditing feature in the Batch Execution Recipe Editor, Equipment Editor, WorkSpace, and WorkInstruction Editor. This feature is not available for the Audit Reporter.

When you configure electronic signatures in the Batch Execution WorkSpace for the Recipe and Equipment Editors, select None as the Default signature type. Similarly, when defining electronic work instruction signature requirements, you can specify the Default Name for Unchecked Properties (the logon name or computer name).

## Determining if a Batch Execution Project or Recipe Has Auditing Enabled

To configure auditing, you use the Electronic Signature tab of the Batch Execution Configuration dialog box in the WorkSpace. Once you enable auditing, a key icon displays in the bottom right corner of the application near the status bar, indicating that you enabled auditing, as shown in the following figure.



Example of Auditing Enabled in the Batch Execution WorkSpace (Equipment Editor)

The auditing key icon displays in the Batch Execution WorkSpace (for the equipment configuration), and in the Batch Execution Equipment and Recipe Editors. If auditing is not enabled, a red restrictive circle appears over the key. The following figure displays examples of how enabled and disabled icons appear in the Batch Execution software.



## Monitoring Product Baselines with Audit Information

When you schedule a batch, Batch Execution stores the recipe and area model audit information, for the recipe and area model that the recipe was saved against, as part of the batch electronic record stored

in the database. This occurs whenever you schedule a batch from the Batch Execution Client, the BatchList or BatchAdd ActiveX control, or through VBIS.

By saving this audit information, you can correlate control recipes with versions of the master recipe and equipment configuration stored in the audit trail database. This helps you by providing validated data for electronic batch records.

Information captured for a control recipe includes:

- Batch ID.
- Computer name on which the Batch Execution Server is running.
- Recipe audit version number and GUID.
- Area model audit version number and GUID.
- Signature information when the main recipe was last saved (user name, user full name, Windows security group, time stamp and optional comment for Performed By or Performed By and Verified By users).
- Signature information when the area model was last saved (user name, user full name, Windows security group, time stamp and optional comment for Performed By or Performed By and Verified By users).

For more detailed information on the table that captures this information, see the BATCH\_AUDIT\_INFO Table section.

---

## Auditing Database Tables

This section describes the tables in which Batch Execution stores the auditing information. These tables include the following:

- BATCH\_AUDIT\_INFO Table
- AUDITTABLE Table
- AUDITREPORTTEMPLATES Table
- BATCH\_CMD\_SIGNATURE\_SUCCESS Table

***NOTE:** The first three auditing tables are described in the sections that follow. The BATCH\_CMD\_SIGNATURE\_SUCCESS table is described in the Custom Applications manual with the other batch event journal database tables. You can click the links above to access any of these sections.*

WorkInstruction stores auditing information in the EWI tables. Electronic signature and auditing capabilities are built-in to the WorkInstruction Editor. For more information refer to the Understanding the WorkInstruction Data Model section in the WorkInstruction Manual.

### Notes on Adding These Tables to Your Database

To add these auditing tables, you must run the appropriate scripts. See the Relational Database Configuration section in the System Configuration manual for more information on database setup and running scripts. If you had a previous version of Batch Execution, refer to the Upgrading Relational Databases in the Upgrade guide.

**BATCH\_AUDIT\_INFO Table**

The BATCH\_AUDIT\_INFO table captures the run-time auditing information. For instance, if auditing is enabled when a batch gets scheduled, audit versioning information gets stored to this table. An audit trail of electronic signatures is also recorded in this table. The following table lists the attributes for the BATCH\_AUDIT\_INFO table.

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
SERVER_NAME	Data Type: String. Length: 64 characters. Null Support: Nulls not allowed. Allowable Values: Windows computer name. Default Value: None. Description: The computer name on which the Batch Execution Server resides.
BATCH_ID	Data Type: String. Length: 128 characters. Null Support: Nulls not allowed. Allowable Values: a-z, A-Z, 0-9, and the underscore character. Default Value: Dependent on user configurations. Description: A user-defined ID that identifies an instance of a control recipe (a batch).
BATCH_SERIAL_NO	Data Type: Integer. Length: 10 digits. Key: Primary Key Component (PK1). Null Support: Nulls not allowed. Allowable Values: Sequential number generated by the Batch Execution Server. This number can range from 0 to 2147483647. Default Value: None. Description: A unique ID that identifies an instance of a control recipe (a batch).

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
RECIPE_ID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Key: Primary key (PK1).</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Default Value: Depends on the procedure type (procedure, unit procedure, or operation).</p> <p>Description: Master recipe ID.</p>
RECIPE_AUDIT_VERSION	<p>Data Type: Integer.</p> <p>Length: 10 digits.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: This number can range from 0 to 2147483647.</p> <p>Description: The audit version number of the recipe file. The audit version number increases by one each time the recipe is saved in the Batch Execution Recipe Editor. However, for recipe files that include sub-recipes, the audit version number of the sub-recipe file does not increment unless there is a change in the sub-recipe itself or in the area model.</p>
AREA_AUDIT_VERSION	<p>Data Type: Integer.</p> <p>Length: 10 digits.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: This number can range from 0 to 2147483647.</p> <p>Description: The audit version number of the area model file. The audit version number increases by one each time the area model is saved in the Batch Execution Equipment Editor.</p>

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AREA_DOCUMENT_UID	<p>Data Type: String.</p> <p>Length: 40 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: A unique, system-generated identifier for the file. Batch Execution generates the globally unique identifier (also known as a GUID) when you save a file for the first time, or use the Save As action to save a file in the Batch Execution Equipment Editor.</p>
RECIPE_DOCUMENT_UID	<p>Data Type: String.</p> <p>Length: 40 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: A unique, system-generated identifier for the file. Batch Execution generates the globally unique identifier (also known as a GUID) when you save a file for the first time, or use the Save As action to save a file in the Batch Execution Recipe Editor.</p>
RECIPE_PERFORMEDBY_USERID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows user name for the person who performed the action. This field is blank if a Performed By signature is not required for this action.</p>
RECIPE_PERFORMEDBY_NAME	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Full name of the person who performed the action. Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Performed By signature is not required for this action.</p>

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
RECIPE_PERFORMEDBY_COMMENT	<p>Data Type: String.</p> <p>Length: 1024 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Comment entered by the person who entered the Performed By electronic signature. This field is blank if the user did not enter a comment or if a Performed By signature is not required for this action.</p>
RECIPE_PERFORMEDBY_TIME	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.</p>
RECIPE_VERIFIEDBY_USERID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows user name for the person who verified the action. This field is blank if a Verified By signature is not required for this action.</p>
RECIPE_VERIFIEDBY_NAME	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Full name of the person who verified the action. Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Verified By signature is not required for this action.</p>

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
RECIPE_VERIFIEDBY_COMMENT	<p>Data Type: String.</p> <p>Length: 1024 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Comment entered by the person who entered the Verified By electronic signature. This field is blank if the user did not enter a comment or if a Verified By signature is not required for this action.</p>
RECIPE_VERIFIEDBY_TIME	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.</p>
AREA_PERFORMEDBY_USERID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows user name for the person who performed the action. This field is blank if a Performed By signature is not required for this action.</p>
AREA_PERFORMEDBY_NAME	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Full name of the person who performed the action. Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Performed By signature is not required for this action.</p>

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AREA_PERFORMEDBY_COMMENT	<p>Data Type: String.</p> <p>Length: 1024 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Comment entered by the person who entered the Performed By electronic signature. This field is blank if the user did not enter a comment or if a Performed By signature is not required for this action.</p>
AREA_PERFORMEDBY_TIME	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.</p>
AREA_VERIFIEDBY_USERID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows user name for the person who verified the action. This field is blank if a Verified By signature is not required for this action.</p>
AREA_VERIFIEDBY_NAME	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Full name of the person who verified the action. Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Verified By signature is not required for this action.</p>

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AREA_VERIFIEDBY_COMMENT	<p>Data Type: String.</p> <p>Length: 1024 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Comment entered by the person who entered the Verified By electronic signature. This field is blank if the user did not enter a comment or if a Verified By signature is not required for this action.</p>
AREA_VERIFIEDBY_TIME	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.</p>
RECIPE_PERFORMEDBY_TIME_UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.</p>

<b>BATCH_AUDIT_INFO Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
RECIPE_VERIFIEDBY_TIME_UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.</p>
AREA_PERFORMEDBY_TIME_UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.</p>
AREA_VERIFIEDBY_TIME_UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.</p>

## AUDITTABLE Table

The AUDITTABLE table captures the design-time auditing information. This table contains auditing information whenever the user performs an audited action in the Recipe Editor, Equipment Editor, Batch Execution Configuration in the WorkSpace, and the WorkInstruction Editor. The following table lists the attributes for the AUDITTABLE table.

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditApplication	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The editor application where the audited action took place. These applications include: Batch Execution Audit Reporter, Batch Execution Electronic Signature Configuration (in the WorkSpace), Batch Execution Equipment Editor, Batch Execution Recipe Editor, GE Batch Execution Equipment Editor (initiated from the WorkSpace), and the WorkInstruction Editor.</p>
AuditApplicationVersion	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The version number of the application where the action took place.</p>
AuditAction	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The action that the user performed. For example, these actions include Startup, Open, Save, Save As, Print, Export, Verify, and so on.</p>

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditActionTimestamp	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user performed the action. The format of this date is: MM/DD/YEAR HR:MN:SC AM/PM. An example of a date is April 22, 2005 16:30:38 PM.</p>
AuditPerformedByUserID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows user name for the person who performed the action. This field is blank if a Performed By signature is not required for this action.</p>
AuditPerformedByFullName	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Full name of the person who performed the action. Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Performed By signature is not required for this action.</p>
AuditPerformedByTimestamp	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.</p>

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditPerformedBySecurityGroup	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows security group for the user who performed the action. This field is blank if a Performed By signature is not required for this action.</p>
AuditPerformedByComment	<p>Data Type: String.</p> <p>Length: 1024 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Comment entered by the person who entered the Performed By electronic signature. This field is blank if the user did not enter a comment or if a Performed By signature is not required for this action.</p>
AuditVerifiedByUserID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows user name for the person who verified the action. This field is blank if a Verified By signature is not required for this action.</p>
AuditVerifiedByFullName	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Full name of the person who verified the action. Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Verified By signature is not required for this action.</p>

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditVerifiedByTimestamp	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: Any valid date.</p> <p>Default Value: The current date and time.</p> <p>Description: The date and time that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.</p>
AuditVerifiedBySecurityGroup	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Windows security group for the user who verified the action. This field is blank if a Verified By signature is not required for this action.</p>
AuditVerifiedByComment	<p>Data Type: String.</p> <p>Length: 1024 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: Comment entered by the supervisor who entered the Verified By electronic signature. This field is blank if the user did not enter a comment or if a Verified By signature is not required for this action.</p>
AuditSignatureType	<p>Data Type: String.</p> <p>Length: 40 characters.</p> <p>Null Support: Nulls not allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The type of signature required for the action: None, Performed By, or Performed By/Verified By.</p>

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditDocumentFilename	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The name and path of the area model, recipe, or XML file (for the EIB) for which the user performed the action.</p>
AuditDocumentVersion	<p>Data Type: Integer.</p> <p>Length: 10 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: This number can range from 0 to 2147483647.</p> <p>Description: The audit version number of the currently configured area model or recipe file. The audit version number increases by one each time the area model or recipe is saved. However, for recipe files that include sub-recipes, the audit version number of the sub-recipe file does not increment unless there is a change in the sub-recipe itself or in the area model.</p>
AuditComputerName	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The name of the Windows computer that the user completed the action on.</p>
AuditLoggedInUserID	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The Windows user name for the user logged in to the computer on which the actions were completed.</p>

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditFixUserName	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The name of the user logged in to the iFIX system on the local computer. This field is blank if a user is not logged in to iFIX when completing the action.</p>
AuditDocumentData	<p>Data Type: Text/BLOB.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: An XML file representation of the recipe (top level only) or area model. When the AuditDocumentData field displays in the Audit Reporter it appears as a paper clip icon, since the field is a BLOB (Binary Large Object) data type and too large to display in the Audit Reporter spreadsheet. The AuditDocumentData field only displays if the AuditAction contains the Save or Save As action. Otherwise, it is blank.</p>
AuditDocumentDataDescription	<p>Data Type: String.</p> <p>Length: 255 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: A string that indicates whether the AuditDocumentData represents a Batch Execution recipe or area model.</p>
AuditDocumentUniqueIdentifier	<p>Data Type: String.</p> <p>Length: 50 characters.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: a-z, A-Z, 0-9, and underscores ( _ ).</p> <p>Description: The unique, system-generated identifier for the file. Batch Execution generates the globally unique identifier (also known as a GUID) when you save a file for the first time, or use the Save As action to save a file.</p>

<b>AUDITTABLE Table</b>	
<b>Attribute</b>	<b>Attribute Description</b>
AuditActionTimestamp.UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user performed the action.</p>
AuditPerformedByTimestamp.UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.</p>
AuditVerifiedByTimestamp.UTC	<p>Data Type: Date.</p> <p>Length: Not applicable.</p> <p>Null Support: Nulls allowed.</p> <p>Allowable Values: A time stamp in UTC format.</p> <p>Default Value: The current date and time, in UTC format.</p> <p>Description: The date and time, in UTC format, that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.</p>

## AUDITREPORTTEMPLATES Table

The AUDITREPORTTEMPLATES table contains the report templates for the Audit Reporter. The following table lists the attributes for the AUDITREPORTTEMPLATES table.

AUDITREPORTTEMPLATES Table	
Attribute	Description
AuditReportTemplateName	Data Type: String. Length: 50 characters. Null Support: Nulls not allowed. Allowable Values: a-z, A-Z, 0-9, and the underscore character. Description: Title for the audit report template.
AuditReportTemplateDescription	Data Type: String. Length: 1024 characters. Null Support: Nulls allowed. Allowable Values: a-z, A-Z, 0-9, and the underscore character. Description: Describes the audit report template.
AuditReportTemplateData	Data Type: BLOB. Null Support: Nulls not allowed. Allowable Values: a-z, A-Z, 0-9, and the underscore character. Description: Contains the Audit Reporter template settings.

---

## Example of an Audit Trail

The following example describes the signature actions and the resulting records generated in the AUDITTABLE in the database when you perform the audited actions in the Recipe Editor. This example displays the records generated when a Performed By signature requirement is configured for all actions.

## **Action 1: Startup**

When you start the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction=Startup
- AuditDocumentFileName= empty
- AuditDocumentVersion=0
- AuditDocumentUniqueIdentifier=NULL
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

## **Action 2: Open**

When you open the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditDocumentVersion=1
- AuditAction=Open
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=3
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

## **Action 3: New**

When you create a new recipe in the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction=New
- AuditDocumentFileName=empty
- AuditDocumentVersion=0
- AuditDocumentUniqueIdentifier=NULL
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

## **Action 4: Print**

When you print a recipe in the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction=Print
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=3
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

### **Action 5: Remove Recipe**

When you remove a recipe in the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction=Delete
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=3
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

### **Action 6: Release to Production**

When you release a recipe to production in the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction=Enable Release Recipe To Production OR  
AuditAction=Disable Release Recipe To Production
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=3
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

### **Action 7: Rebuild a Recipe Directory**

When you rebuild a recipe directory in the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction= Rebuild All Recipes
- AuditDocumentFileName= empty
- AuditDocumentVersion=0

- AuditDocumentUniqueIdentifier=NULL
- AuditDocumentData=NULL
- AuditDocumentDataDescription=NULL

### Action 8: Save a Recipe Without Verifying

When you save a recipe without verifying in the Recipe Editor, a Performed By signature request appears. The AUDITTABLE generates a record that contains:

- AuditAction=Save
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=4  
*NOTE: The AuditDocumentVersion field is incremented when you save the file.*
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=<long text>
- AuditDocumentDataDescription= Batch Execution Recipe

### Action 9: Save a Recipe, Accept and then Cancel the Verification of the Electronic Signature

When you save and verify a recipe, but cancel the electronic signature for the verification the Recipe Editor, the AUDITTABLE generates a record that contains:

- AuditAction=Save
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=4  
*NOTE: The AuditDocumentVersion field gets incremented when you save the file.*
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=<long text>
- AuditDocumentDataDescription= Batch Execution Recipe

### Action 10: Save and Verify a Recipe

When you save and verify a recipe, Batch Execution verifies and saves the current recipe and sub-recipes. Batch Execution generates a save recipe record and a verify recipe record for each recipe. The AUDITTABLE record contains one or more save records, and one or more verified recipe records.

## Action 11: Verify but Not Save a Recipe

When you verify a recipe and cancel the save, Batch Execution cancels the verify recipe operation. The verify command requires you to save updated recipes to the recipe storage. Since the recipe header fields get updated, you cannot perform a verify without performing a save command.

## Action 12: Verify and Save a Recipe

When you verify and save a recipe, Batch Execution performs the verify recipe operation on the current recipe and all sub-recipes. The results are displayed in the Verification Results dialog box. All verified recipes get saved to storage. All saved recipes have audit information updated, which means Batch Execution increments the audit version number.

***NOTE:** The sub-recipe's audit version is not incremented if the sub-recipe or area model does not contain changes. In that case, the sub-recipe retains its original audit version number, while the current recipe audit version number is incremented.*

The AUDITTABLE record contains one or more verify recipe records and one or more save recipe records.

A verified recipe record contains:

- AuditAction=Verify
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=4

***NOTE:** The AuditDocumentVersion field gets incremented when you save the file.*

- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription= NULL

## Action 13: Verify All Recipes

This action functions like action 12, except that this command closes any recipes that are open and verifies all recipes in the recipe.dir file. You issue this command from Verify All Recipes menu option in the File menu of the Recipe Editor.

## Action 14: Save As

This action functions the same as actions 8, 9, and 10. You enter a new file name in the Recipe Save As dialog box when you use the Save As command. Upon a successful save, the audit record contains:

- AuditAction=Save As
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_GEL.BPC
- AuditDocumentVersion=1
- AuditDocumentUniqueIdentifier= F24F649E87E04AFA9DB4E0D0D5C11F2E

- AuditDocumentData=<long text>
- AuditDocumentDataDescription= Batch Execution Recipe

### **Action 15: Convert Project Storage and Cancel the Electronic Signature**

When you convert the project storage and then cancel the electronic signature, Batch Execution cancels the convert project storage operation. The convert recipe storage operation saves updated recipes to the recipe storage. That is why a save recipe command is required while converting recipes.

### **Action 16: Convert Project Storage and Accept the Electronic Signature**

When you convert the project storage and then accept the electronic signature, Batch Execution performs the convert project storage operation on all recipes. All saved recipes contain updated audit information and Batch Execution increments the audit version number.

The AUDITTABLE generates one or more records for each saved recipe. Each record contains:

- AuditAction=Convert Recipe Storage
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=5  
*NOTE: Note this field gets incremented during save.*
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription= NULL

### **Action 17: Upgrade Recipes and Cancel the Electronic Signature**

When you choose to upgrade recipes but cancel the electronic signature, Batch Execution cancels the upgrade operation. The Recipe Editor closes if you tried to open a recipe when opening the Recipe Editor.

The upgrade recipe operation saves the updated recipes to the recipe storage. That is why a save recipe operation requires an electronic signature to upgrade one or more recipes.

### **Action 18: Upgrade Recipes and Accept the Electronic Signature**

When you choose to upgrade recipes and accept the electronic signature, Batch Execution performs the upgrade operation on all recipes. When you open the Recipe Editor, it automatically detects that the recipes are not the current version.

All saved recipes contain updated audit information and the audit version is incremented for each recipe.

The AUDITTABLE record contains one or more upgrade recipe records and one or more save recipe records.

An upgrade recipe record contains:

- AuditAction= Upgrade
- AuditDocumentFileName= F:\Program Files\Proficy\Proficy Batch Execution\PROJECTS\DEMO\RECIPES\MAKE\_TOO.BPC
- AuditDocumentVersion=0
- AuditDocumentUniqueIdentifier= E7B3B3A610D04EAA81DB1CA7DEAD3220
- AuditDocumentData=NULL
- AuditDocumentDataDescription= NULL

***NOTE:** The upgrade record contains an audit version of 0, and the corresponding Save data record contains an audit version of 1.*

---

## Audit Reporter Dialog Boxes

The Audit Reporter application includes the following dialog boxes for use with auditing (listed in alphabetical order):

- Data Source Configuration Dialog Box
- Datasources Dialog Box
- Electronic Signature Dialog Box
- Page Setup Dialog Box
- Report Template Dialog Box

### Data Source Configuration Dialog Box

The Data Source Configuration dialog box displays the following items:

#### **DSN**

Enter the name of the ODBC data source that contains the AuditTable, or click Browse to select a data source.

#### **Browse**

Click to browse for a data source.

#### **User Name**

Enter the name of the user who has access to the database where the AuditTable is located.

#### **Password**

Enter the password for the user who has access to the database where the AuditTable is located.

## Datasources Dialog Box

The Data Source Configuration dialog box displays the following item:

### Data Source List

Displays a list of the available data sources.

**NOTE:** The Audit Reporter does not support the Oracle ODBC Driver because it doesn't implement all the required features. Oracle users should use the Microsoft ODBC for Oracle driver instead.

## Electronic Signature Dialog Box

The Electronic Signature dialog box displays the following item:

### Enable Authority Check

Select this check box if you want a Windows user name and password to be required every time a user opens the Audit Reporter or extracts document data from a saved recipe or area model. When you click OK, Proficy Batch Execution requests a user name and password from the Windows iESigAdministrators group to accept the configuration.

Each time a user enters a user name and password from the Audit Reporter, it is tracked in the Audit Trail.

## Page Setup Dialog Box

The Page Setup dialog box displays the following items:

### Layout Example

Shows how the page layout will look. As you change the options, the page layout example changes.

### Paper Group

The following table lists the items contained in the Paper group:

Item	Description
Size	Specifies the size of the paper, envelope, or other print media you want to use.
Source	Specifies where the paper you want to use is located in the printer. Different printer models support different paper sources, such as the upper tray, envelope feed, and manual feed.

## Orientation Group

Specifies how the document is positioned on the printed page.

To see how the orientation will look on the sample page, click Portrait or Landscape.

## Margins (Inches)

Sets the printing area of the page. The printer will print only within these margins.

## Report Template Dialog Box

The Report Template dialog box displays the following items:

### Label Tab

The following table lists the input fields to edit the labels for the report:

Item	Description
Author	Enter the name of the report author.
Title	Enter a title for the report.
Description	Enter a description for the report. You can enter up to 800 characters, including spaces. To create a new line insert a /n field code before the text you want to appear on the next line.
Header	Enter the text, if any, that you want to appear in the header of the printed report. You can enter up to 80 characters per line including spaces, and a total of 850 characters for the entire field.  To create a new line insert a /n field code before the text you want to appear on the next line.
Footer	Enter the text, if any, that you want to appear in the footer of the printed report. You can enter up to 80 characters per line including spaces, and a total of 850 characters for the entire field.  To create a new line insert a /n field code before the text you want to appear on the next line.
AutoText	Allows you to insert a new line, align text (left, right, or center), add the author, title, time stamp, or description, change the font, or include a page count.

## Columns Tab

The following table lists the columns tab editing options:

Item	Description
Columns Table	Displays the available columns and column titles that you display in a report.
Move Up Button	Select a column and click this button to move it up in the report's column display order. <i>NOTE: When a column is selected, it displays as bolded text.</i>
Move Down Button	Select a column and click this button to move it down in the report's column display order. <i>NOTE: When a column is selected, it displays as bolded text.</i>
Show Button	Select a column and click this button to make it visible in the report.
Hide Button	Select a column and click this button, if you do not want to display this column in the report output. <i>NOTE: When a column is selected, it displays as bolded text.</i>
Defaults Button	Click to restore the default column display options.

## Criteria Tab

The following table lists the criteria tab editing options:

Item	Description
Criteria Table	Displays the columns for which you can define querying criteria.
Defaults Button	Click to restore the default querying criteria.

## Sort Tab

The following table lists the sorting options:

<b>Item</b>	<b>Description</b>
Available Columns List	Displays a list of available columns to sort by.
Add Button	Select an available column and then click this button to add it to the list of selected columns to sort by.
Add All Button	Click to add all available columns to the list of selected columns to sort by.
Remove Button	Select a column from the selected column list and click this button to remove it.
Remove All Button	Click to remove all of the selected columns from the list on the right.
Up Arrow Button	Click this button to move the selected column up in the list of sorting priority.
Down Arrow Button	Click this button to move the selected column down in the list of sorting priority.
Selected Columns List	Displays a list of selected columns that you want to sort by.
Sort This Column Drop Down	Select the order that you want the selected columns to be sorted by: ascending or descending order.

---

## How Do I...

The following sections explain how to work with the Audit Reporter:

- Using Shortcuts in the Audit Reporter
- Performing Basic Operations in the Audit Reporter
- Working with Reports
- Running Reports
- Modifying Report Viewing Formats

- Modifying Report Display Options
- Printing Reports
- Optimizing Reports

## Shortcuts in the Audit Reporter

### ►To run a report:

Press F5 or click the Run Report button in the toolbar.

### ►To resize columns or rows:

Click and drag the column or row divider.

### ►To print a report:

Press Ctrl+P or click the Print button in the toolbar.

## Performing Basic Operations in the Audit Reporter

For information on performing basic operations in the Audit Reporter, refer to the following sections:

- Starting the Audit Reporter
- Configuring a Data Source
- Entering a Data Source
- Displaying a Report in the Audit Reporter
- Using Electronic Signatures in the Audit Reporter
- Retrieving the .XML Version of a Saved Document
- Summary of Database Columns You Can Report on

### Starting the Audit Reporter

#### ►To start the Audit Reporter:

1. On the Start menu, point to Programs, Proficiency Batch Execution, and then click WorkSpace. The Proficiency Batch Execution WorkSpace application appears.
2. In the WorkSpace toolbar, click the Audit Reporter icon.  
- Or -  
In the WorkInstruction Editor, on the Options menu, click Audit Reporter.
3. The Proficiency Batch Execution Audit Reporter application appears.

## Configuring a Data Source

### ►To configure the data source:

1. In the Audit Reporter, on the Tools menu, point to Options, and then click DSN Configuration. The Data Source Configuration dialog box appears.
2. In the DSN field, enter the data source name or click the Browse button to select a data source from the list in the Datasources dialog box.
3. In the User Name field, enter a user name.
4. In the Password field, enter a password.

**IMPORTANT:** *The user name and password field must contain a value; these fields cannot be left empty.*

5. Click OK.

#### **NOTES:**

- *You must have the DSN for the audit trail database configured before you can enter it in the DSN field. To configure the DSN, use the ODBC Data Source Administrator dialog box. You can access this dialog box from the Control Panel's Administrative Tools folder by clicking the Data Sources (ODBC) icon.*
- *The Audit Reporter does not support the Oracle ODBC Driver because it doesn't implement all the required features. Oracle users should use the Microsoft ODBC for Oracle driver instead.*

## Entering a Data Source

### ►To enter the data source:

1. In the Audit Reporter, on the Tools menu, point to Options, and then click DSN Configuration. The Data Source Configuration dialog box appears.
2. In the DSN field, enter the data source name or click the Browse button to select a data source from the list in the Datasources dialog box.
3. In the User Name field, enter a user name.
4. In the Password field, enter a password.

**NOTE:** *The user name and password field must contain a value; these fields cannot be left empty.*

5. Click OK.

#### **NOTES:**

- *You must have the DSN for the audit trail database configured before you can enter it in the DSN field. To configure the DSN, use the ODBC Data Source Administrator dialog box. You can access this dialog box from the Control Panel's Administrative Tools folder by clicking the Data Sources (ODBC) icon.*
- *The Audit Reporter doesn't support the Oracle ODBC Driver because it doesn't implement all the required features. Oracle users should use the Microsoft ODBC for Oracle driver instead.*

## Displaying a Report in the Audit Reporter

### ►To display a report in the Audit Reporter:

1. In the Audit Reporter, select the data source from which you want to retrieve data:
  - a. In the Audit Reporter, on the Tools menu, point to Options, and then click DSN Configuration. The Data Source Configuration dialog box appears.
  - b. In the DSN field, enter the data source name or click the Browse button to select a data source from the list.
  - c. In the User Name field, enter a user name.
  - d. In the Password field, enter a password.  
***IMPORTANT:** The user name and password field must contain a value; these fields cannot be left empty.*
  - e. Click OK.
2. Open the Report Template dialog box to review the displayed columns and search criteria. Change settings as required:
  - a. On the Report menu, click Template. The Report Template dialog box appears.
  - b. Click the Columns tab.
  - c. Inspect the database fields in the list, and decide what fields to display:
    - If you want to hide a column in the report, click the database field and then click Hide.
    - If you want to show a column in the report, click the database field and then click Show.
    - If you want to move a displayed field, click the database field you want to move then click the Move Up or Move Down button to position it in the location you want.
    - If you want to restore the defaults, click the Default button. When you click Default, all columns display except the AuditDocumentData and AuditDocumentDataDescription fields. When a database field is selected, it appears in Bolded text.
  - d. If you want to change the criteria used to return the columns, use the Criteria tab in the Report Template dialog box.
  - e. Click OK.
  - f. Run the report again to view the results of the changes.
  - g. Optionally, save the report template for future use.
3. On the Report menu, click Run, or click the Run button.
4. Wait a few seconds for data to populate in the Audit Reporter spreadsheet. The amount of time that you wait depends upon the size of the results returned by the query.

***TIP:** You can shorten the wait time by adding search criteria from the Report Template dialog box.*

## Using Electronic Signatures in the Audit Reporter

### ►To enable electronic signatures in the Audit Reporter:

1. In the Audit Reporter, on the Tools menu, point to Options, and then click Electronic Signatures. The Electronic Signatures dialog box appears.
2. Select the Enable Authority Check check box.
3. Click OK.

When you enable authority checks in the Audit Reporter, Proficy Batch Execution requires a user name and password from the iESigAdministrators Windows security group. After you enable it, you must enter a user name and password from the AuditReporterUsers Windows security group when you start the Audit Report, or extract the document data from a saved recipe or area model.

## Retrieving the .XML Version of a Saved Document

### ►To open the XML version of a saved document file:

1. In the Audit Reporter, make sure that the AuditDocumentData column displays in your report output:
  - On the Report menu, click Template. The Report Template dialog box appears.
  - Click the Columns tab and scroll to the end of the list of database fields.
  - Make sure a check box appears next to the AuditDocumentData column.
2. Run the report.
3. Select the row from which you want to obtain the XML version of the document.

You can only obtain an XML version of the document for rows that are the result of a Save or Save As action in the Recipe, Equipment Editor, or WorkSpace. The Audit Reporter displays paperclips in the Document Data field of these rows.

4. On the Report menu, click Retrieve Document. The Retrieve Document dialog box appears.

**NOTE:** You can also double-click the AuditDocumentData field to display the Retrieve Document dialog box.

5. Enter the name that you want to save the XML document as in the File Name field.
6. Select a location to save the file to.
7. Click OK.
8. Browse to the folder you saved the file to in the Windows Explorer to view the XML document.

## Summary of Database Columns You Can Report on

The following list outlines descriptions of the database columns that display in the Audit Reporter:

- AuditApplication** – the application where the design-time audited action took place. These applications include: Batch Execution Audit Reporter, Batch Execution Electronic Signature Configuration (in the WorkSpace), Batch Execution Equipment Editor, Batch Execution Recipe Editor, Batch Execution Equipment Editor (initiated from the WorkSpace), and the WorkInstruction Editor.
- AuditApplicationVersion** – the version number of the application where the action took place.
- AuditAction** – the action that the user performed. For example, these actions include Startup, Open, Save, Save As, Print, Export, Validate, and so on.
- AuditActionTimestamp** – the date and time that the user performed the action. The format of this date is: MM/DD/YEAR HR:MN:SC AM/PM. An example of a date is as follows: May 22, 2005 16:30:38 PM.
- AuditPerformedByUserId** – Windows user name for the person who performed the action. This field is blank if a Performed By signature is not required for this action.
- AuditPerformedByFullName** – full name of the person who performed the action. Proficiency Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Performed By signature is not required for this action.
- AuditPerformedByTimeStamp** – date and time that the user entered the Performed By signature. This field is blank if a Performed By signature is not required for this action.
- AuditPerformedBySecurityGroup** – Windows security group for the user who performed the action. This field is blank if a Performed By signature is not required for this action.
- AuditPerformedByComment** – comment entered by the operator who entered the Performed By electronic signature. This field is blank if the user did not enter a comment or if a Performed By signature is not required for this action.
- AuditVerifiedByUserId** – Windows user name for the person who verified the action. This field is blank if a Verified By signature is not required for this action.
- AuditVerifiedByFullName** – full name of the person who verified the action. Proficiency Batch Execution does not accept a signature without a full user name defined in Windows security. This field is blank if a Verified By signature is not required for this action.
- AuditVerifiedByTimeStamp** – date and time that the user entered the Verified By signature. This field is blank if a Verified By signature is not required for this action.
- AuditVerifiedBySecurityGroup** – Windows security group for the user who verified the action. This field is blank if a Verified By signature is not required for this action.
- AuditVerifiedByComment** – comment entered by the supervisor who entered the Verified By electronic signature. This field is blank if the user did not enter a comment or if a Verified By signature is not required for this action.

**AuditSignatureType** – the type of signature required for the action: None, Performed By, or Performed By/Verified By.

**AuditDocumentFilename** – name and path of the area model, recipe, or XML file (for the EIB) for which the user performed the action.

**AuditDocumentVersion** – the audit version number of the currently configured area model or recipe file. The audit version number increases by one each time the area model or recipe is saved.

**AuditComputerName** – the name of the Windows computer that the user completed the action on.

**AuditLoggedInUserId** – the Windows user name for the user logged in to the computer from which the actions were completed.

**AuditFixUserName** – the name of the user logged in to the iFIX system on the local computer. This field is blank if a user is not logged in to iFIX when completing the action.

**AuditDocumentData** – an XML file representation of the recipe (top level only) or area model. When the AuditDocumentData field displays in the Audit Reporter it appears as a paperclip icon, since the field is a BLOB (Binary Large Object) data type and too large to display in the Audit Reporter spreadsheet. The AuditDocumentData field only displays if the AuditAction contains the Save or Save As action. Otherwise, it is blank. If a paperclip appears in this field, you can double-click it to retrieve the XML document.

**AuditDocumentDataDescription** – a string that indicates whether the AuditDocumentData represents a Proficiency Batch Execution Recipe or Equipment Model.

**AuditDocumentUniqueIdentifier** – the unique, system-generated identifier for the file. Proficiency Batch Execution generates the globally unique identifier (also known as a GUID) when you save a file for the first time, or use the Save As action to resave a file.

## Working With Reports

For information on working with reports in the Audit Reporter, refer to the following sections:

- Defining How a Report is Sorted
- Defining the Criteria Used When Running a Report
- Configuring which Columns Display in a Report
- Configuring the Report Template Properties
- Saving a Report Template
- Exporting a Report

## Defining How a Report is Sorted

### ►To define how a report is sorted:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Sort tab.
3. In the Available Columns list, select the column that you want to sort by.
4. Click Add to include that column in the Selected Columns list for sorting. You can also double-click the selected row to move it to the Selected Columns list.
5. Repeat steps 3-4 for each column that you want to sort by.
6. To change the sorting order of a column in the list, select the column name and use the Up and Down arrows to position it in the list.

The sorting priority is defined by the order that the columns appear in the Selected Column list. The Audit Reporter sorts the results by the first column in the list, followed by the second column, and then the third column, and so on (for as many columns that you included in the list).

7. To change the sort direction of a column, select a column and then select in Ascending or Descending Order from the Sort this Column drop-down list.

**TIP:** Double-click a column to change the sorting order from Ascending to Descending or Descending to Ascending. By default, all columns display in Ascending Order.

8. Click OK.
9. Run the report again to view the results of the changes.
10. Optionally, save the report template for future use.

## Defining the Criteria Used When Running a Report

### ►To define the criteria used when running a report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. Click the database field for which you want to define the return criteria.

**NOTE:** When a database field is selected, it appears in *Bolded text*.

4. Select the operator that you want to use from the drop-down list.
5. Enter a value or values for which you want to perform the operation, or select one from the drop-down list, if available. For all operators except BETWEEN, multiple values are interpreted with the Boolean OR expression.
6. Repeat steps 3-5 for each database field to which you want to assign criteria.
7. Run the report again to view the results of the changes.
8. Double-click an EWI or Logic Step in the grid. The EWI Editor or Logic Step Editor dialog box appears.
9. Optionally, save the report template for future use.

## Configuring which Columns Display in a Report

### ►To configure which columns display in a report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Columns tab.
3. Inspect the database fields in the list, and decide what fields to display:
  - If you want to hide a column in the report, click the database field and then click Hide.
  - If you want to show a column in the report, click the database field and then click Show.
  - If you want to move a displayed field, click the database field you want to move then click the Move Up or Move Down button to position it in the location you want.
  - If you want to restore the defaults, click the Default button. When you click Default, all columns display except the AuditDocumentData and AuditDocumentDataDescription fields.

*NOTE: When a database field is selected, it appears in Bolded text.*

4. If you want to change the criteria used to return the columns, use the Criteria tab in the Report Template dialog box.
5. Click OK.
6. Run the report again to view the results of the changes.
7. Optionally, save the report template for future use.

## Configuring the Report Template Properties

### ►To configure the report template properties:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. From the Report Template dialog box, click the Label tab.
3. In the Author field, enter the name of the person who created the report template.
4. In the Title field, enter the name for the report.
5. In the Description field, enter a brief description. You can enter up to 800 characters, including spaces.
6. In the Header field, enter the text for the header. You can enter up to 80 characters per line, and a total of 850 characters for the entire field.
7. In the Footer field, enter the text for the footer. You can enter up to 80 characters per line, and a total of 850 characters for the entire field.

*TIP: You can insert field codes into either the Header or Footer fields, by using the Autotext button next to the field. If an entire line when printing exceeds 80 characters, the Audit Reporter truncates the line at the 81st character. To create a new line, insert a /n field code before the text you want to appear on the new line.*

8. Click OK.

**NOTE:** You can configure the header and footer information before or after you run the report. The Audit Reporter saves the header and footer information into a report template.

Entering text in any of the fields for the Label tab is optional.

## Saving a Report Template

For information on saving a report template in the Audit Reporter, refer to the following sections:

- Saving the Report Template
- Renaming the Report Template
- Exporting a Report to a File

### Saving the Report Template

#### ►To save the report:

1. In the Audit Reporter, on the File menu, click Save. If a template is not already open, the Save Template As dialog box appears.
2. In the Template Name field, enter a name.
3. Click Save.

**NOTE:** You do not need to run a report to configure and save report template settings.

### Renaming the Report Template

#### ►To save the report template under another name:

1. In the Audit Reporter, on the File menu, click Save As. The Save Template As dialog box appears.
2. In the Template Name field, enter a name.
3. Click Save.

**NOTE:** You do not need to run a report to configure and re-save report template settings.

### Exporting the Report to View as an .XML File

#### ►To export a report:

1. In the Audit Reporter, run the report.
2. On the Report menu, click Export. The Export Report dialog box appears.
3. In the File Name field, enter a name for the exported file and select a location to save the file.
4. From the Save File as Type drop-down list, select a type: XML file, Excel Worksheet, or HTML file.

**NOTE:** If you save the report as an HTML file, realize that the report may take longer to

*generate than the other formats. For example, if your report contains hundreds of rows, it could take many hours to generate.*

5. Click OK.

## **Exporting a Report**

For information on exporting a report in the Audit Reporter, refer to the following sections:

- Exporting as an XML File
- Exporting as a Microsoft Excel Worksheet File
- Exporting as an HTML File

### **Exporting a Report as an XML File**

#### **►To export the report as an XML file:**

1. In the Audit Reporter, run the report.
2. On the Report menu, click Export. The Export Report dialog box appears.
3. In the File Name field, enter a name for the exported file, and select a location to save the file.
4. From the Save File as Type drop-down list, select XML File.
5. Click OK.

### **Exporting as a Microsoft Excel Worksheet File**

#### **►To export the report as a Microsoft Excel file:**

1. In the Audit Reporter, run the report.
2. On the Report menu, click Export. The Export Report dialog box appears.
3. In the File Name field, enter a name for the exported file and select a location to save the file.
4. From the Save File as Type drop-down list, select Excel File.
5. Click OK.

The Audit Reporter exports the file for Microsoft Excel in BIFF8 format, which you can open in Microsoft Excel 97, 2000, or 2002.

### **Exporting a Report as an HTML File**

#### **►To export the report as an HTML file:**

1. In the Audit Reporter, run the report.
2. On the Report menu, click Export. The Export Report dialog box appears.
3. In the File Name field, enter a name for the exported file and select a location to save the file.
4. From the Save File as Type drop-down list, select HTML Files.

**NOTE:** If you save the report as an HTML file, realize that the report may take longer to generate than the other formats. For example, if your report contains hundreds of rows, it could take many hours to generate.

5. Click OK.

## Running Reports

For information on running reports in the Audit Reporter, refer to the following sections:

- Displaying a Report in the Audit Reporter
- Waiting for a Report to Run
- Optimizing Query Performance
- Shortcuts in the Audit Reporter

### Displaying a Report in the Audit Reporter

#### ►To display a report in the Audit Reporter:

1. In the Audit Reporter, select the data source from which you want to retrieve data:
  - a. In the Audit Reporter, on the Tools menu, point to Options, and then click DSN Configuration. The Data Source Configuration dialog box appears.
  - b. In the DSN field, enter the data source name or click the Browse button to select a data source from the list.
  - c. In the User Name field, enter a user name.
  - d. In the Password field, enter a password.
 

**IMPORTANT:** The user name and password field must contain a value; these fields cannot be left empty.
  - e. Click OK.
3. Open the Report Template dialog box to review the displayed columns and search criteria. Change settings as required:
  - e. On the Report menu, click Template. The Report Template dialog box appears.
  - f. Click the Columns tab.
  - g. Inspect the database fields in the list, and decide what fields to display:
    - If you want to hide a column in the report, click the database field and then click Hide.
    - If you want to show a column in the report, click the database field and then click Show.
    - If you want to move a displayed field, click the database field you want to move then click the Move Up or Move Down button to position it in the location you want.
    - If you want to restore the defaults, click the Default button. When you click Default, all columns display except the AuditDocumentData and

AuditDocumentDataDescription fields. When a database field is selected, it appears in Bolded text.

- a. If you want to change the criteria used to return the columns, use the Criteria tab in the Report Template dialog box.
  - b. Click OK.
  - c. Run the report again to view the results of the changes.
  - d. Optionally, save the report template for future use.
3. On the Report menu, click Run, or click the Run button.
  4. Wait a few seconds for data to populate in the Audit Reporter spreadsheet. The amount of time that you wait depends upon the size of the results returned by the query.

***TIP:** You can shorten the wait time by adding search criteria from the Report Template dialog box.*

### Waiting for a Report to Run

#### ►To wait for a report to run:

Be aware that:

- The more columns that you request, the longer the query takes.
- The less search criteria that you use, the more time the query takes.
- The progress bar indicates how much longer you must wait for the query to finish executing.
- The Cancel button stops the query. The Audit Reporter displays any records retrieved so far.

### Optimizing Query Performance

#### ►To optimize query performance:

- Use the Columns tab in the Report Template dialog box to optimize the number of rows returned.
- Use the Criteria tab in the Report Template dialog box to optimize the number of rows returned.

### Examples of Using the Criteria Tab to Optimize Performance

- Use a minimal time period, by specifying a date range in the ActionTimestamp column.
- Use the Criteria tab in the Report Template dialog box to optimize the number of rows returned.
- Be specific about the application for which you want to check the audit trail, by specifying the application in the AuditApplication column.
- Be specific about the signature type for which you want to check report on, by specifying the

signature type in the AuditSignatureType column.

- Return all rows that contain text or do not contain text for a specific column.

## Modifying Report Viewing Formats

For information on report viewing formats in the Audit Reporter, refer to the following sections:

- Displaying a Report in the Audit Reporter
- Printing the Report to View on Paper
- Exporting the Report to View as an .XML File

### Displaying a Report in the Audit Reporter

#### ►To display a report in the Audit Reporter:

1. In the Audit Reporter, select the data source from which you want to retrieve data:
  - a. In the Audit Reporter, on the Tools menu, point to Options, and then click DSN Configuration. The Data Source Configuration dialog box appears.
  - b. In the DSN field, enter the data source name or click the Browse button to select a data source from the list.
  - c. In the User Name field, enter a user name.
  - d. In the Password field, enter a password.  
***IMPORTANT:** The user name and password field must contain a value; these fields cannot be left empty.*
  - e. Click OK.
3. Open the Report Template dialog box to review the displayed columns and search criteria. Change settings as required:
  - e. On the Report menu, click Template. The Report Template dialog box appears.
  - f. Click the Columns tab.
  - g. Inspect the database fields in the list, and decide what fields to display:
    - If you want to hide a column in the report, click the database field and then click Hide.
    - If you want to show a column in the report, click the database field and then click Show.
    - If you want to move a displayed field, click the database field you want to move then click the Move Up or Move Down button to position it in the location you want.
    - If you want to restore the defaults, click the Default button. When you click Default, all columns display except the AuditDocumentData and AuditDocumentDataDescription fields. When a database field is selected, it appears in Bolded text.
  - a. If you want to change the criteria used to return the columns, use the Criteria tab in the Report Template dialog box.

- b. Click OK.
  - c. Run the report again to view the results of the changes.
  - d. Optionally, save the report template for future use.
3. On the Report menu, click Run, or click the Run button.
4. Wait a few seconds for data to populate in the Audit Reporter spreadsheet. The amount of time that you wait depends upon the size of the results returned by the query.

***TIP:** You can shorten the wait time by adding search criteria from the Report Template dialog box.*

## Printing a Report

### ►To print a report:

1. In the Audit Reporter, run the report.
2. Optionally, configure the header and footer for the printed report.
3. On the File menu, click Print. The Print dialog box appears.
4. Click OK.

## Exporting the Report to View as an .XML File

### ►To export a report:

1. In the Audit Reporter, run the report.
2. On the Report menu, click Export. The Export Report dialog box appears.
3. In the File Name field, enter a name for the exported file and select a location to save the file.
4. From the Save File as Type drop-down list, select a type: XML file, Excel Worksheet, or HTML file.

***NOTE:** If you save the report as an HTML file, realize that the report may take longer to generate than the other formats. For example, if your report contains hundreds of rows, it could take many hours to generate.*

5. Click OK.

## Modifying Report Display Options

For information on report display options in the Audit Reporter, refer to the following sections:

- Defining How a Report is Sorted
- Defining the Criteria Used When Running a Report
- Configuring which Columns Display in a Report
- Adjusting the Row or Column Width
- Changing the Column Names
- Defining Font Properties

## Defining How a Report is Sorted

### ►To define how a report is sorted:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Sort tab.
3. In the Available Columns list, select the column that you want to sort by.
4. Click Add to include that column in the Selected Columns list for sorting. You can also double-click the selected row to move it to the Selected Columns list.
5. Repeat steps 3-4 for each column that you want to sort by.
6. To change the sorting order of a column in the list, select the column name and use the Up and Down arrows to position it in the list.

The sorting priority is defined by the order that the columns appear in the Selected Column list. The Audit Reporter sorts the results by the first column in the list, followed by the second column, and then the third column, and so on (for as many columns that you included in the list).

7. To change the sort direction of a column, select a column and then select in Ascending or Descending Order from the Sort this Column drop-down list.

***TIP:** Double-click a column to change the sorting order from Ascending to Descending or Descending to Ascending. By default, all columns display in Ascending Order.*

8. Click OK.
9. Run the report again to view the results of the changes.
10. Optionally, save the report template for future use.

## Defining the Criteria Used When Running a Report

### ►To define the criteria used when running a report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. Click the database field for which you want to define the return criteria.

***NOTE:** When a database field is selected, it appears in Bolded text.*

4. Select the operator that you want to use from the drop-down list.
5. Enter a value or values for which you want to perform the operation, or select one from the drop-down list, if available. For all operators except BETWEEN, multiple values are interpreted with the Boolean OR expression.
6. Repeat steps 3-5 for each database field to which you want to assign criteria.
7. Run the report again to view the results of the changes.
8. Double-click an EWI or Logic Step in the grid. The EWI Editor or Logic Step Editor dialog box appears.
9. Optionally, save the report template for future use.

## Configuring which Columns Display in a Report

### ►To configure which columns display in a report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Columns tab.
3. Inspect the database fields in the list, and decide what fields to display:
  - If you want to hide a column in the report, click the database field and then click Hide.
  - If you want to show a column in the report, click the database field and then click Show.
  - If you want to move a displayed field, click the database field you want to move then click the Move Up or Move Down button to position it in the location you want.
  - If you want to restore the defaults, click the Default button. When you click Default, all columns display except the AuditDocumentData and AuditDocumentDataDescription fields.

*NOTE: When a database field is selected, it appears in Bolded text.*

4. If you want to change the criteria used to return the columns, use the Criteria tab in the Report Template dialog box.
5. Click OK.
6. Run the report again to view the results of the changes.
7. Optionally, save the report template for future use.

## Adjusting the Row or Column Width

### ►To adjust the row or column width:

1. In the Audit Reporter, run the report.
2. Place your cursor in the heading where the column titles or row numbers appear.
3. Move your cursor over the line below the row or to the right of the column that you want to expand. The cursor changes to a split bar.
4. Click and drag the split bar to the desired location.

## Changing the Column Names Displayed for the Report

### ►To change the column names displayed for the report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Columns tab.
3. Select the column that you want to change the name of. When the column is selected, it displays in Bolded text.

4. Double-click the Display Name field for the selected column.
5. Enter the new name.
6. Repeat steps 3-5 for each column that you want to change the name of.

***NOTE:** Make sure that the Visible check box is selected for each column title that you want to change; if the Visible check box is not selected, the column does not display in the report output.*

7. Run the report again.

## Defining Font Properties

### ►To define the font properties:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. On the Label tab, click an AutoText button, and select Font. The Font dialog box appears.
3. In the Font list, select a font name.
4. From the second list box, select a Font style.
5. In the third list box, select a point size for the font.
6. Click OK.

## Printing Reports

For information on printing reports in the Audit Reporter, refer to the following sections:

- Printing a Report
- Configuring the Header and Footer for a Printed Report
- Changing the Page Setup for the Printed Report

### Printing a Report

#### ►To print a report:

1. In the Audit Reporter, run the report.
2. Optionally, configure the header and footer for the printed report.
3. On the File menu, click Print. The Print dialog box appears.
4. Click OK.

## Configuring the Header and Footer for a Printed Report

### ►To configure the header and footer for a printed report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. From the Label tab, enter the text for the header in the Header field. You can enter up to 80 characters per line, and a total of 850 characters for the entire field.
3. In the Footer field, enter the text for the footer. You can enter up to 80 characters per line, and a total of 850 characters for the entire field.

***TIP:** You can insert field codes into either the Header or Footer fields, by using the Autotext button next to the field. If an entire line when printing exceeds 80 characters, the Audit Reporter truncates the line at the 81st character. To create a new line, insert a /n field code before the text you want to appear on the new line.*

4. Click OK.

***NOTE:** You can configure the header and footer information before or after you run the report. The Audit Reporter saves the header and footer information into a report template.*

## Changing the Page Setup for the Printed Report

### ►To change the page setup, including layout, for a report:

1. In the Audit Reporter, on the File menu, click Page Setup. The Page Setup dialog box appears.
2. Change the Orientation to Landscape if you prefer to include more columns per page.
3. Additionally, change the page size, source, or margins to fit the needs of your printer.
4. Click OK.
5. On the File menu, click Print. The Print dialog box appears.
6. Click OK.

## Optimizing Reports

For information on report optimization tips in the Audit Reporter, refer to the following sections:

- Changing the Number of Columns Displayed
- Defining Search Criteria to Limit the Number of Returned Rows
- Defining a Date Range for Returned Rows
- Specifying an Application to Limit Returned Rows
- Specifying a Signature Type to Return Data for
- Specifying NULL or not-NULL Columns

## Configuring which Columns Display in a Report

### ►To configure which columns display in a report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Columns tab.
3. Inspect the database fields in the list, and decide what fields to display:
  - If you want to hide a column in the report, click the database field and then click Hide.
  - If you want to show a column in the report, click the database field and then click Show.
  - If you want to move a displayed field, click the database field you want to move then click the Move Up or Move Down button to position it in the location you want.
  - If you want to restore the defaults, click the Default button. When you click Default, all columns display except the AuditDocumentData and AuditDocumentDataDescription fields.

*NOTE: When a database field is selected, it appears in Bolded text.*

4. If you want to change the criteria used to return the columns, use the Criteria tab in the Report Template dialog box.
5. Click OK.
6. Run the report again to view the results of the changes.
7. Optionally, save the report template for future use.

## Defining the Criteria Used When Running a Report

### ►To define the criteria used when running a report:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. Click the database field for which you want to define the return criteria.

*NOTE: When a database field is selected, it appears in Bolded text.*

4. Select the operator that you want to use from the drop-down list.
5. Enter a value or values for which you want to perform the operation, or select one from the drop-down list, if available. For all operators except BETWEEN, multiple values are interpreted with the Boolean OR expression.
6. Repeat steps 3-5 for each database field to which you want to assign criteria.
7. Run the report again to view the results of the changes.
8. Double-click an EWI or Logic Step in the grid. The EWI Editor or Logic Step Editor dialog box appears.
9. Optionally, save the report template for future use.

## Defining a Date Range for Returned Rows

### ►To define a date range for the returned rows:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. In the Database Field list, click ActionTimestamp.
4. Select Between from the Operator drop-down list for the ActionTimestamp.
5. Double-click the first value field for the ActionTimestampOn.
6. Enter a date that you want to begin the range on, in the format of MM/DD/YYYY or MON DD, YYYY. You can also write out the month. For example, these dates are both acceptable: 05/22/05 and May 22, 2005. You can also include the time in the Value field. For example, you format a valid date and time as follows: 20:05:28 May 30, 2005.
7. Double-click the second value field for the ActionTimestamp.
8. In the second Value field, enter a date that you want to end the range on.
9. Click OK.
10. Run the report again to view the results of the changes.

## Specifying an Application to Limit Returned Rows

### ►To limit the returned rows by specifying an application:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. Click AuditApplication in the Database Field list.
4. Select Equal To from the Operator drop-down list for the AuditApplication.
5. Double-click the first value field for the AuditApplication.
6. Select the application that you want to obtain audit data for from the drop-down list.

These values include: Batch Execution Audit Reporter, Batch Execution Electronic Signature Configuration (in the WorkSpace), Batch Execution Equipment Editor, Batch Execution Recipe Editor, Batch Execution Equipment Editor (initiated from the WorkSpace), and the WorkInstruction Editor.

7. Click OK.
8. Run the report again to view the results of the changes.

## Specifying a signature type to return data

### ►To specify a signature type to return data:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. In the Database Field list, click AuditSignatureType.
4. Select Equal To from the Operator drop-down list for the AuditSignatureType.
5. Double-click the first value field for the AuditSignatureType.
6. Select the signature type that you want to obtain audit data for from the drop-down list. These values include: Performed By and Performed By/Verified By.
7. Click OK.
8. Run the report again to view the results of the changes.

## Specifying NULL or not-NULL columns

### ►To specify NULL or not-NULL columns:

1. In the Audit Reporter, on the Report menu, click Template. The Report Template dialog box appears.
2. Click the Criteria tab.
3. Click the database field for which you want to define the return criteria.  
*NOTE: For more information, refer to the Overview of Database Fields section.*
4. Select the Equal To or Not Equal To operator from the drop-down list for the selected database field.
5. Double-click the first value field for the selected database field.
6. Enter the following text, including angle brackets: <NULL>
7. Click OK.
8. Run the report again to view the results of the changes.



---

# Index

## A

accounts .....	13	audit trail.....	28
actions available for signing		audit versioning overview.....	28
ActiveX controls.....	6	audited document.....	29
Audit Reporter .....	8	auditing	
Equipment Editor.....	6	determining whether enabled.....	37
Recipe Editor.....	5	enabling .....	35
actions available for signing .....	5	without capturing signatures.....	36
ActiveX controls		auditing .....	36
actions available for signing .....	6	auditing database tables .....	38
ActiveX controls.....	6	AUDITREPORTTEMPLATES table.....	54
adding operators and supervisors		AUDITTABLE table .....	47
Windows XP.....	11	automatic versioning of area models and recipes.....	28
adding operators and supervisors .....	11	<b>B</b>	
audit		BATCH_AUDIT_INFO table .....	39
information on product baselines.....	37	<b>C</b>	
audit.....	37	captured audited fields.....	29
Audit Reporter		comments with an electronic signature.....	24
actions available for signing .....	8	configuring	
using to view the audit trail .....	32	auditing .....	36
Audit Reporter.....	32	electronic signatures .....	14
audit trail		configuring .....	14
data stored.....	33	configuring auditing	
example .....	54	Audit Reporter .....	36
understanding .....	28	Recipe and Equipment Editors .....	36

configuring auditing .....	36
creating user accounts.....	13
<b>D</b>	
Data Source Configuration dialog box .....	60, 61
design-time audit information	
example .....	32
overview .....	31
design-time audit information .....	31
determining a signed action.....	5
determining whether auditing enabled.....	37
<b>E</b>	
Electronic Signature dialog box .....	61
electronic signatures	
comments.....	24
configuration overview.....	15
configuring .....	14
configuring in the ActiveX Controls .....	19
configuring in the Audit Reporter .....	20
configuring in the Recipe and Equipment Editors .....	16
examples .....	22
guidelines.....	4
introduction .....	1
overview .....	2
performing .....	21
using .....	3
electronic signatures .....	3
enabling auditing .....	35

Equipment Editor	
actions available for signing .....	6
configuring auditing .....	36
Equipment Editor.....	36
errors	
failed signing attempts.....	25
errors.....	25
examples	
audit trail.....	54
electronic signatures .....	22
Performed By signature .....	22
Performed By signature in the ActiveX Controls .....	24
Performed By/Verified By signature .....	23
Performed By/Verified By signature in the ActiveX Controls .....	25
viewing design-time audit information.....	32
Windows security configuration.....	11
XML schema .....	34
examples .....	34
<b>F</b>	
failed signing attempts.....	25
<b>G</b>	
guidelines	
working with electronic signatures .....	4
guidelines.....	4
<b>I</b>	
iFIX security .....	18
introduction to electronic signatures.....	1

<b>L</b>		Controls .....	24
license and key checking .....	15	Performed By/Verified By.....	23
<b>M</b>		Performed By/Verified By signature in the ActiveX Controls .....	25
monitoring product baselines.....	37	signature types .....	25
<b>O</b>		signed action determination.....	5
overview		<b>T</b>	
electronic signature configuration .....	15	tables	
electronic signatures .....	2	AUDITREPORTTEMPLATES.....	54
using electronic signatures.....	3	AUDITTABLE.....	47
overview .....	3	BATCH_AUDIT_INFO .....	39
<b>P</b>		tables.....	39
Page Setup dialog box .....	61	tracking electronic signatures .....	9
Performed By signature .....	22	<b>U</b>	
Performed By signature in the ActiveX Controls .....	24	understanding	
Performed By/Verified By signature .....	23	audit versioning and the audit trail .....	28
Performed By/Verified By signature in the ActiveX Controls.....	25	Windows security and electronic signatures .....	10
performing electronic signatures .....	21	understanding .....	10
<b>R</b>		user accounts .....	13
Recipe Editor		using	
actions available for signing .....	5	Audit Reporter .....	32
configuring auditing .....	36	electronic signatures .....	3
Recipe Editor.....	36	using .....	3
Report Template dialog box .....	62	<b>V</b>	
<b>S</b>		viewing	
signature types		audited XML documents .....	34
Performed By .....	22	design-time audit information.....	31
Performed By signature in the ActiveX		viewing .....	31

**W**

Windows security

- example ..... 11
- groups ..... 12
- overview ..... 10

Windows security ..... 10

Windows XP

- adding operators and supervisors..... 11

Windows XP..... 11

**X**

XML schema example ..... 34