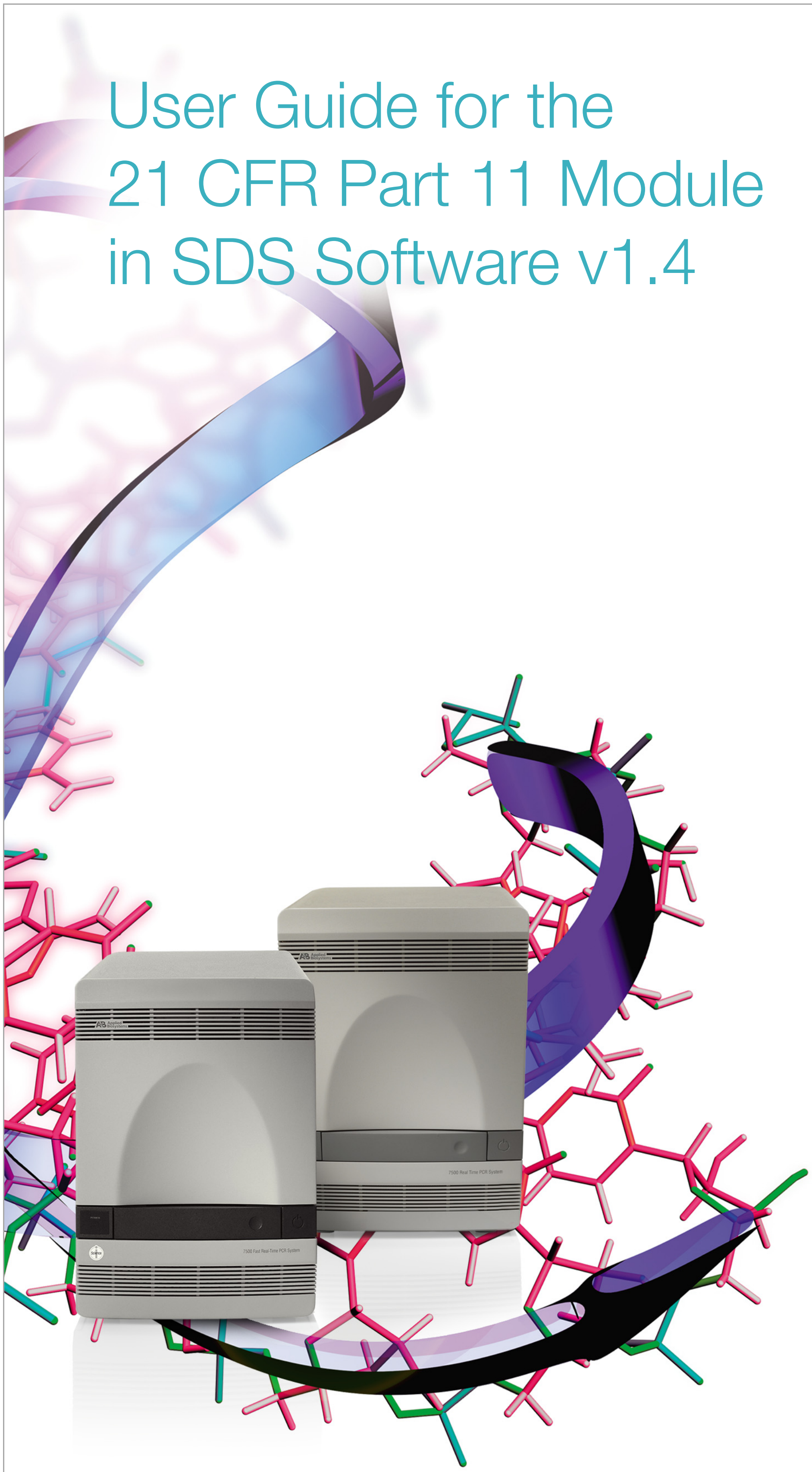
Applied Biosystems 7500/7500 Fast
Real-Time PCR System

User Guide for the 21 CFR Part 11 Module in SDS Software v1.4



1 Introduction

2 Installation

3 Logging in to the SDS Software

4 Configuring the 21CFR11 Module

5 Audit Trails

6 E-Signatures

7 Controlled Activities

© Copyright 2006, 2010 Applied Biosystems. All rights reserved.

For Research Use Only. Not for use in diagnostic procedures.

Information in this document is subject to change without notice. Applied Biosystems assumes no responsibility for any errors that may appear in this document.

APPLIED BIOSYSTEMS DISCLAIMS ALL WARRANTIES WITH RESPECT TO THIS DOCUMENT, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THOSE OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL APPLIED BIOSYSTEMS BE LIABLE, WHETHER IN CONTRACT, TORT, WARRANTY, OR UNDER ANY STATUTE OR ON ANY OTHER BASIS FOR SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, MULTIPLE OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING FROM THIS DOCUMENT, INCLUDING BUT NOT LIMITED TO THE USE THEREOF.

NOTICE TO PURCHASER:

The Applied Biosystems 7500 and 7500 Fast Real-Time PCR Systems are real-time thermal cyclers covered by US patents and corresponding claims in their non-US counterparts, owned by Applied Biosystems. No right is conveyed expressly, by implication or by estoppel under any other patent claim, such as claims to apparatus, reagents, kits, or methods such as 5′ nuclease methods. Further information on purchasing licenses may be obtained by contacting the Director of Licensing, Applied Biosystems, 850 Lincoln Centre Drive, Foster City, California 94404, USA.

TRADEMARKS:

AB (Design) and Applied Biosystems are registered trademarks and Applera is a trademark of Applied Biosystems or its subsidiaries in the U.S. and/or certain other countries.

Microsoft, PowerPoint, and Windows are registered trademarks of Microsoft Corporation.

All other trademarks are the sole property of their respective owners.

Part Number 4374432 Rev. C
06/2010

Contents

Preface v

How to Use This Guide v
How to Obtain More Information vii
How to Obtain Support viii

Chapter 1 Introduction 1

Overview 2
Important Compliance Information 4
Best Practices 5

Chapter 2 Installation 7

Required User Privileges for the Activities in this Chapter 8
Selecting the Installation Method 8
Installing with the Real-Time System Setup Wizard 9
Creating Users and User Groups in the Operating System 12

Chapter 3 Logging in to the SDS Software 23

Logging in to the SDS Software 24
Multiple User Accounts on the Same Computer 27

Chapter 4 Configuring the 21CFR11 Module 31

Before You Begin 32
Overview 32
Configuring the Idle Timeout 33
Configuring User Group Permissions 35
Configuring Data Auditing 37
Configuring E-Signatures 40

Chapter 5 Audit Trails 45

Before You Begin 46
Overview 46
Recording Changes in the Individual Audit Trails 48

Viewing Audit Trails 49

Chapter 6 E-Signatures 57

Before You Begin 58

Overview 58

Recording E-Signatures 63

Viewing E-Signatures 66

Chapter 7 Controlled Activities 71

Overview 72

Analyze Data File 73

Calibrate System 73

Configure System 74

Create SDS File 74

Delete SDS File 75

Export Results 75

Export Setup 76

Manage Run List 77

Perform Function Test 78

Print Report 78

Save SDS File 79

Start Run 79

Stop Run 80

View Audit History 80

Glossary 81

Index 85

Preface

How to Use This Guide

Purpose of This Guide

The 21 CFR Part 11 module can be purchased as an enhancement to the Sequence Detection Systems (SDS) Software for the Applied Biosystems 7500/7500 Fast Real-Time PCR System. The purpose of this guide is to describe:

- The installation and management tasks related to the 21 CFR Part 11 module.
- The features of the 21 CFR Part 11 module that users in the laboratory may encounter.

Note: This guide does not describe the general features of the SDS Software. Use this guide in conjunction with the SDS Software documentation and Help System listed under "How to Obtain More Information" on page vii.

Audience

This guide is written for:

- System administrators who install and manage the SDS Software (Chapter 2 and Chapter 4).
- Laboratory staff running assays with the SDS Software. Features of the 21 CFR Part 11 module that may affect laboratory staff are audit trails, E-Signatures, and Controlled Activities (Chapter 5, Chapter 6, and Chapter 7).

Assumptions

This guide assumes that you have:

- Familiarity with the Microsoft® Windows® XP operating system.
- A general understanding of hard drives and data storage, file transfers, and copying and pasting.
- Familiarity with the SDS Software.

Text Conventions

This guide uses the following conventions:

- **Bold** indicates user action. For example:

  Type **0**, then press **Enter** for each of the remaining fields.
- *Italic* text indicates new or important words and is also used for emphasis. For example:

  Before analyzing, *always* prepare fresh matrix.
- A right arrow bracket (>) separates successive commands you select from a drop-down or shortcut menu. For example:

  Select **File ▸ Open**.

User Attention Words

The following user attention words appear in Applied Biosystems user documentation. Each word implies a particular level of observation or action as described below:

Note – Provides information that may be of interest or help but is not critical to the use of the product.

IMPORTANT! – Provides information that is necessary for proper instrument operation, accurate chemistry kit use, or safe use of a chemical.

⚠ **CAUTION** Indicates a potentially hazardous situation that, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices.

⚠ **WARNING** Indicates a potentially hazardous situation that, if not avoided, could result in death or serious injury.

Safety

Chemical manufacturers supply current Material Safety Data Sheets (MSDSs) with shipments of hazardous chemicals to *new* customers. They also provide MSDSs with the first shipment of a hazardous chemical to a customer after an MSDS has been updated. MSDSs provide the safety information you need to store, handle, transport, and dispose of the chemicals safely.

Each time you receive a new MSDS packaged with a hazardous chemical, be sure to replace the appropriate MSDS in your files.

You can obtain from Applied Biosystems the MSDS for any chemical supplied by Applied Biosystems. This service is free and available 24 hours a day.

To obtain MSDSs:

1. Go to **https://docs.appliedbiosystems.com/msdssearch.html**.
2. In the Search field, type in the chemical name, part number, or other information that appears in the MSDS of interest. Select the language of your choice, then click **Search**.
3. Find the document of interest, right-click the document title, then select any of the following:
    - **Open** – To view the document
    - **Print Target** – To print the document
    - **Save Target As** – To download a PDF version of the document to a destination that you choose
4. To have a copy of a document sent by fax or e-mail, select **Fax** or **Email** to the left of the document title in the Search Results page, then click **RETRIEVE DOCUMENTS** at the end of the document list.
5. After you enter the required information, click **View/Deliver Selected Documents Now**.

Refer to the *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Installation and Maintenance Getting Started Guide* and the *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Site Preparation Guide* for important safety information.

How to Obtain More Information

Related Documentation

For information about using the 7500/7500 Fast Real-Time PCR System, refer to the documents listed below.

Note: The documents listed below do not provide information about the 21CFR11 module.

- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Online Help*
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Absolute Quantitation Using Standard Curve Getting Started Guide* (PN 4347825)
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Allelic Discrimination Getting Started Guide* (PN 4347822)
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Plus/Minus Getting Started Guide* (PN 4347821)
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Relative Quantitation Using Comparative C_T Getting Started Guide* (PN 4347824)
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Installation and Maintenance Guide* (PN 4347828)
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Site Preparation Guide* (PN 4347823)
- *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Performing Fast Gene Quantification Quick Reference Card* (PN 4362285)
- *Real-Time PCR Systems Computer Setup Guide* (PN 4365367)
- *Real-Time PCR Systems Chemistry Guide* (PN 4348358)

Obtaining Information from the Help System

The 7500/7500 Fast Real-Time PCR System has a Help system that describes how to use each feature of the user interface. Access the Help system by doing one of the following:

- Click ? in the toolbar of the SDS Software window
- Select **Help ▸ Contents and Index**
- Press **F1**

You can use the Help system to find topics of interest by:

- Reviewing the table of contents
- Searching for a specific topic
- Searching an alphabetized index

You can also access PDF versions of all documents in the 7500/7500 Fast Real-Time PCR System document set from the Help system.

Note: The Help system provides only general information about the 21CFR11 module user interface.

Send Us Your Comments

Applied Biosystems welcomes your comments and suggestions for improving its user documents. You can e-mail your comments to:

techpubs@appliedbiosystems.com

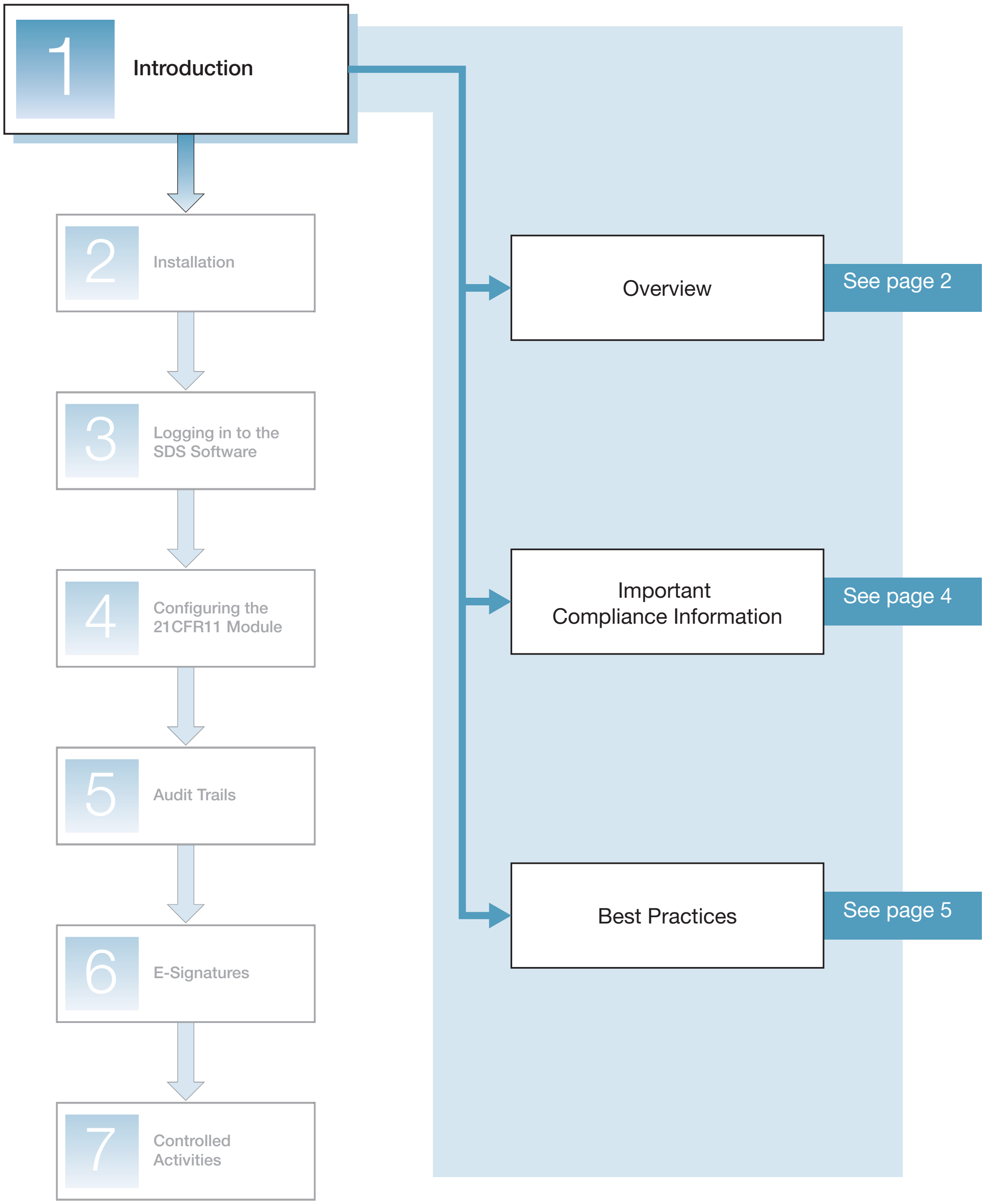
How to Obtain Support

For the latest services and support information for all locations, go to **http://www.appliedbiosystems.com**, then click the link for **Support**.

At the Support page, you can:

- Obtain worldwide telephone and fax numbers to contact Applied Biosystems Technical Support and Sales facilities
- Search through frequently asked questions (FAQs)
- Submit a question directly to Technical Support
- Order Applied Biosystems user documents, MSDSs, certificates of analysis, and other related documents
- Download PDF documents
- Obtain information about customer training
- Download software updates and patches

1 Introduction



Notes

Overview

The 21 CFR Part 11 module (21CFR11 module) can be purchased as an enhancement to Sequence Detection Systems (SDS) Software v1.4 for the Applied Biosystems 7500/7500 Fast Real-Time PCR System. The 21CFR11 module can assist users in complying with FDA Title 21 Code of Federal Regulations Part 11. FDA Title 21 Code of Federal Regulations Part 11 regulates electronic records and electronic signatures.

Features

The 21CFR11 module in SDS Software v1.4 provides the features listed below.

Category	Features
Security	The security features prevent unauthorized access to the SDS Software by:
	• Authenticating each user's login information.
	• Automatically locking out access and requiring reauthentication if a user remains inactive for a set period of time.
	• Logging any unauthorized attempts to access the SDS Software in the Event Log.
	• Verifying each user's permission to perform predefined Controlled Activities.
	• Detecting changes to SDS data that have occurred outside of the SDS Software. The SDS Software will not open any file that has been altered without using the SDS Software.
E-Signatures	The E-Signatures features regulate electronic signing by:
	• Verifying each user's permission to record an E-Signature.
	• Recording E-Signatures for predefined Signing Types.
	• When an E-Signature is *required* for a Signing Type, restricting the actions users can perform if a current E-Signature is not recorded.
	• Including all current E-Signatures when data are printed or exported.
Data auditing	The data auditing features track changes to SDS data by:
	• Storing audit trails to independently record the date and time users create, delete, or update SDS data.
	• Allowing users to review the audit trails.
Instrument	The instrument features determine the validity of source data by:
	• Authenticating that the connected instrument is an Applied Biosystems 7500/7500 Fast Real-Time PCR System.
	• Recording the instrument's serial number. **Note:** You must enter your instrument's serial number in the SDS Software during software installation. You can then view the serial number from within the SDS Software as follows: In the SDS Software main menu, select **Instrument** ▶ **Serial Number** to open the Instrument window, then select the **Configuration** tab (default).

Configurable Features

An SDS Software System Administrator can tailor the following features of the 21CFR11 module to support your company's Standard Operating Procedures (SOPs) and controls:

- **Idle timeout** – The amount of time a user can remain inactive (no mouse or keyboard activity) before the SDS Software automatically logs the user out.
- **User Group Permissions** – The authorization each User Group has to perform predefined Controlled Activities.
- **Data auditing** – The File Types that maintain audit trails, when to prompt for an audit trail comment, and whether a comment entry is optional or required.
- **E-Signatures** – The File Types that maintain E-Signatures and whether an E-Signature is optional or required for predefined Signing Types.

For more information, see Chapter 4, "Configuring the 21CFR11 Module," on page 31.

File Types

The File Types discussed in this document are described in the table below.

File Type	Description	Data is stored in...
User Runs	SDS Documents created by users.	*.sds files
User Studies	SDS Multi-Plate Documents created by users.	*.sdm files
Templates	SDS Templates created by users.	*.sdt files
System Configuration	Configuration data used by the system. This includes configuration data for the 21CFR11 module, system analysis parameters, and hardware.	—
System Calibration	Calibration data collected from a 7500/7500 Fast instrument and used by the SDS Software. **Note:** Each 7500/7500 Fast instrument generates its own calibration data. Each instrument's calibration data should be applied only to assays performed on that instrument.	—
System Run List	References to all User Runs and User Studies created in or imported into the SDS Software.	—

Notes

Important Compliance Information

The 21CFR11 module in SDS Software v1.4, in conjunction with your company's SOPs, can assist you in complying with FDA Title 21 Code of Federal Regulations Part 11. You must ensure that all parts of the FDA regulation are followed. Compliance may include (but is not necessarily limited to):

- Validating your Real-Time PCR System.
- Controlling access to and use of your system documentation.
- Determining that the system users have the education, training, and experience required to perform their assigned tasks.
- Verifying the identity of each user.
- Restricting user accounts appropriately.
- Checking or revising user account passwords periodically.
- Performing loss management procedures to deauthorize compromised accounts.
- Certifying to the FDA the use of electronic records and electronic signatures.
- Configuring the SDS Software 21CFR11 module consistently with your intended use.
- Establishing and following conforming SOPs.

Note: For suggestions on establishing SOPs, see "Best Practices" on page 5.

For More Information

For more information on complying with the FDA Title 21 Code of Federal Regulations Part 11, refer to the FDA website:

http://www.fda.gov

Notes

Best Practices

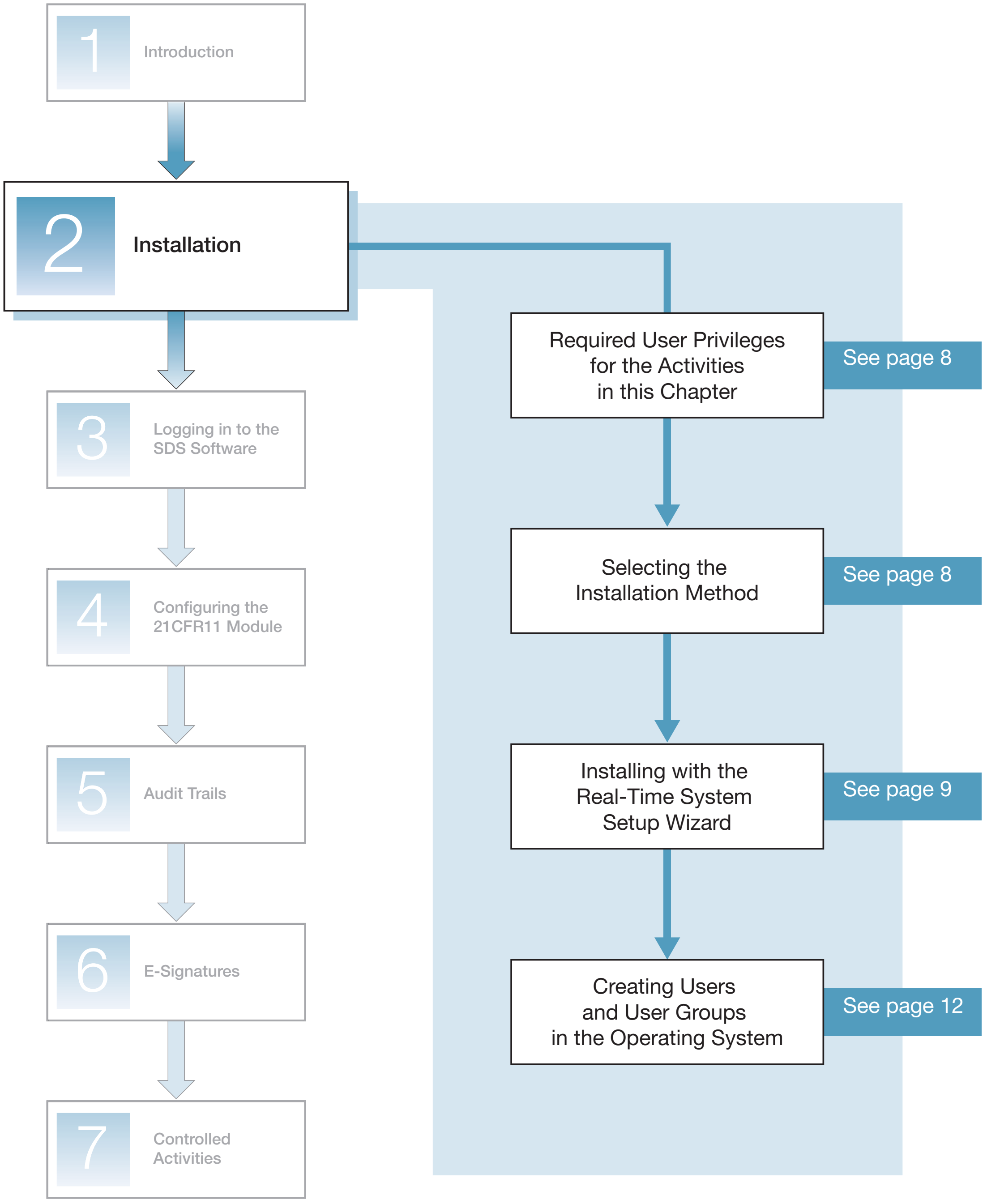
Your company may wish to consider the Best Practices listed below when establishing its SOPs.

Category	Best Practice
E-Signatures	Establish policies to periodically check the SDS Software Event Log in order to detect unauthorized E-Signature attempts.
	Establish policies that hold individuals accountable and responsible for fraudulent actions initiated under their E-Signature.
Microsoft® Windows® XP operating system security	Establish policies for using the Windows Audit Policies tool to audit the Windows System Event Log of account logon events, account management events, audit policy changes, and object access events.
	Establish account lockout policies, using the Security Settings in your Windows XP operating system.
	Establish policies for maintaining defunct user names by disabling user accounts instead of deleting user accounts. Disabling user accounts guarantees unique user names and prevents the reuse and/or reassignment of user names to individuals.
	Establish a policy that all user passwords expire within a period dictated by your risk level. Use the Security Settings in your Windows XP operating system to enforce your policy.
	Establish policies to set the Windows XP operating system time on the computer to prevent alteration without proper controls.
SDS data	Establish policies for archiving and backing up SDS data that are submitted to the government.
	Establish a policy for creating SDS data in secure folders (that is, file system directories with limited access permissions).
	Establish a policy NOT to manage or manipulate SDS data outside of the SDS Software.
Training	Establish training policies for users of SDS Software v1.4.
Virus control	Establish policies for using virus scan software to add protection against undesired alterations of SDS data. **Note:** Applied Biosystems recommends that you do not schedule virus scanning to occur during a run.

Notes

Notes

2 Installation


1 Introduction
2 Installation
3 Logging in to the SDS Software
4 Configuring the 21CFR11 Module
5 Audit Trails
6 E-Signatures
7 Controlled Activities
Required User Privileges for the Activities in this Chapter
See page 8
Selecting the Installation Method
See page 8
Installing with the Real-Time System Setup Wizard
See page 9
Creating Users and User Groups in the Operating System
See page 12

Notes

Required User Privileges for the Activities in this Chapter

You must belong to the Administrators group in the Microsoft® Windows® XP operating system to perform the activities in this chapter.

Selecting the Installation Method

You can install your Real-Time PCR System using one of the following:

- (Recommended) The Real-Time System Setup Wizard on the Installation CD.

  The Real-Time System Setup Wizard guides you through all of the procedures required to install/upgrade your Real-Time PCR System, including the procedures required to install the 21 CFR Part 11 module. See "Installing with the Real-Time System Setup Wizard" on page 9.
- (Not recommended) The *Applied Biosystems 7300/7500/7500 Fast Real-Time PCR System Installation and Maintenance Guide*.

  The *Installation and Maintenance Guide* provides procedures for a standard installation/upgrade, but does not include the procedures required to install the 21 CFR Part 11 module. If you choose to install/upgrade using the *Installation and Maintenance Guide*, you will also need to perform the following procedures in this User Guide in order to use the 21CFR11 module:
  - "Creating Users and User Groups in the Operating System" on page 12
  - "Configuring the 21CFR11 Module" on page 31

Notes

Installing with the Real-Time System Setup Wizard

The Real-Time System Setup Wizard is a software tool that you can use to install or upgrade your Real-Time PCR System. The wizard includes the following installation procedures for the 21 CFR Part 11 module:

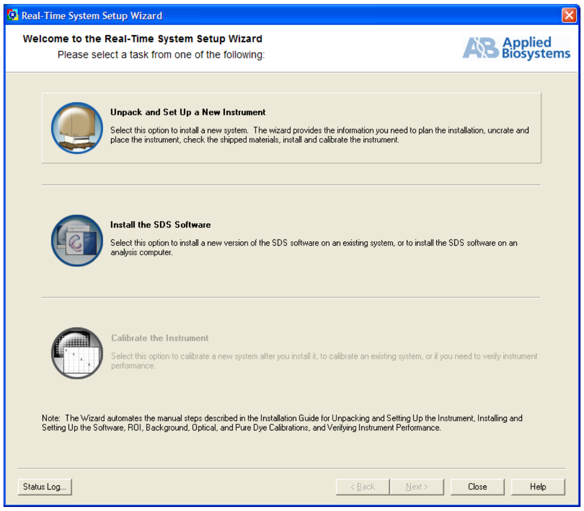
- Registering the product.
- Creating users and User Groups in the Windows XP operating system.
- Configuring the 21CFR11 module.

Note: These procedures are briefly summarized in step 4 on page 10.

1. Set up the computer and log in to the Windows XP operating system as a Windows Computer Administrator, as described in the *Applied Biosystems Real-Time PCR System Computer Setup Guide*.

2. Insert the Software CD in the computer CD drive. The wizard starts automatically after a short delay.

   If the wizard does not automatically start, double-click 🖥 (**My Computer**), navigate to the CD drive, then double-click **SystemSetupWizard.exe**.



Welcome to the Real-Time System Setup Wizard

Please select a task from one of the following:

Unpack and Set Up a New Instrument

Select this option to install a new system. The wizard provides the information you need to plan the installation, uncrate and place the instrument, check the shipped materials, install and calibrate the instrument.

Install the SDS Software

Select this option to install a new version of the SDS software on an existing system, or to install the SDS software on an analysis computer.

Calibrate the Instrument

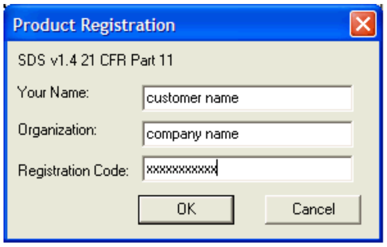
Select this option to calibrate a new system after you install it, to calibrate an existing system, or if you need to verify instrument performance.

Note: The Wizard automates the manual steps described in the Installation Guide for Unpacking and Setting Up the Instrument, Installing and Setting Up the Software, ROI, Background, Optical, and Pure Dye Calibrations, and Verifying Instrument Performance.

3. Select the appropriate installation procedure:
   - If this is a new installation, click **Unpack and Set Up a New Instrument**.
   - If this is a software upgrade, click **Install the SDS Software**.

4. Follow the wizard instructions. If you purchased the SDS Software with the 21CFR11 module, the wizard instructs you to:

   a. Complete the Product Registration dialog box for the 21 CFR Part 11 module. The registration code can be found on the SDS Software CD case.



Product Registration

SDS v1.4 21 CFR Part 11

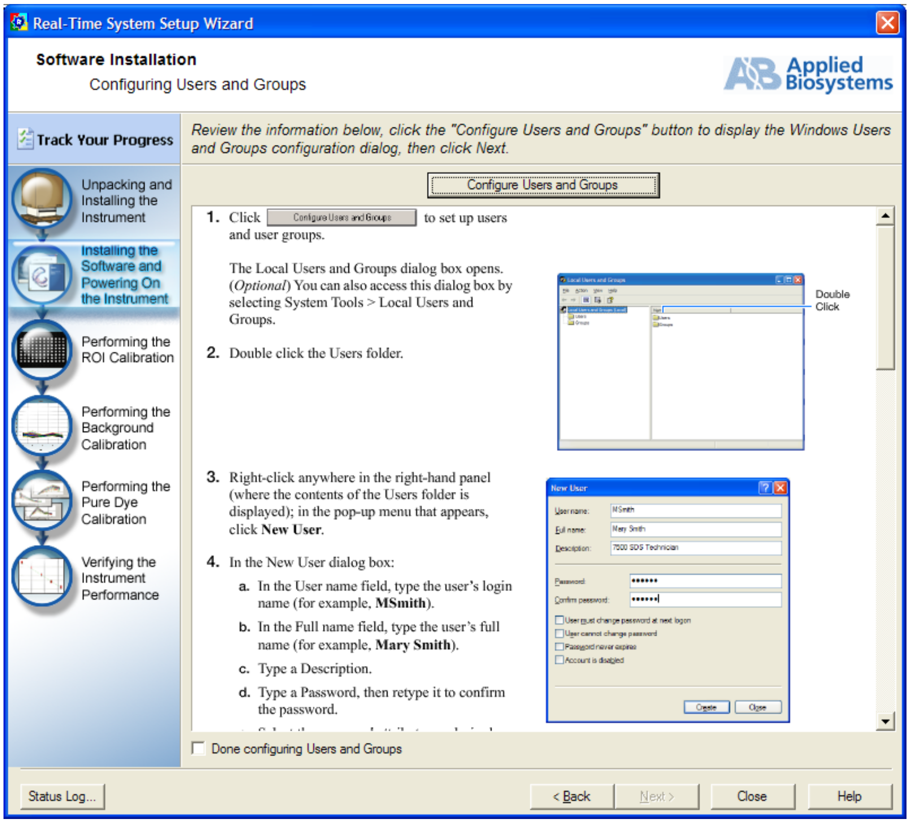
Your Name: customer name

Organization: company name

Registration Code: xxxxxxxxxxx

   b. Create SDS Software User Groups in the Windows XP operating system (**Configure Users and Groups** button).

IMPORTANT! To complete all of the installation procedures, you will need to configure the 21CFR11 module, perform functional testing, and run the RNase P Verification plate. Be sure to add your user account to an SDS Software User Group (or Groups) that has permission to perform the *Analyze Data File, Calibrate System, Configure System, Create SDS File, Perform Function Test, Save SDS File,* and *Start Run* Controlled Activities.



Real-Time System Setup Wizard

Software Installation

Configuring Users and Groups

Applied Biosystems
Track Your Progress
Unpacking and Installing the Instrument
Installing the Software and Powering On the Instrument
Performing the ROI Calibration
Performing the Background Calibration
Performing the Pure Dye Calibration
Verifying the Instrument Performance

Review the information below, click the "Configure Users and Groups" button to display the Windows Users and Groups configuration dialog, then click Next.

Configure Users and Groups

1. Click Configure Users and Groups to set up users and user groups.

   The Local Users and Groups dialog box opens. (*Optional*) You can also access this dialog box by selecting System Tools > Local Users and Groups.

2. Double click the Users folder.

3. Right-click anywhere in the right-hand panel (where the contents of the Users folder is displayed); in the pop-up menu that appears, click **New User**.

4. In the New User dialog box:

   a. In the User name field, type the user's login name (for example, **MSmith**).

   b. In the Full name field, type the user's full name (for example, **Mary Smith**).

   c. Type a Description.

   d. Type a Password, then retype it to confirm the password.

New User

User name: MSmith

Full name: Mary Smith

Description: 7500 SDS Technician

Password: ••••••

Confirm password: ••••••

□ User must change password at next logon

□ User cannot change password

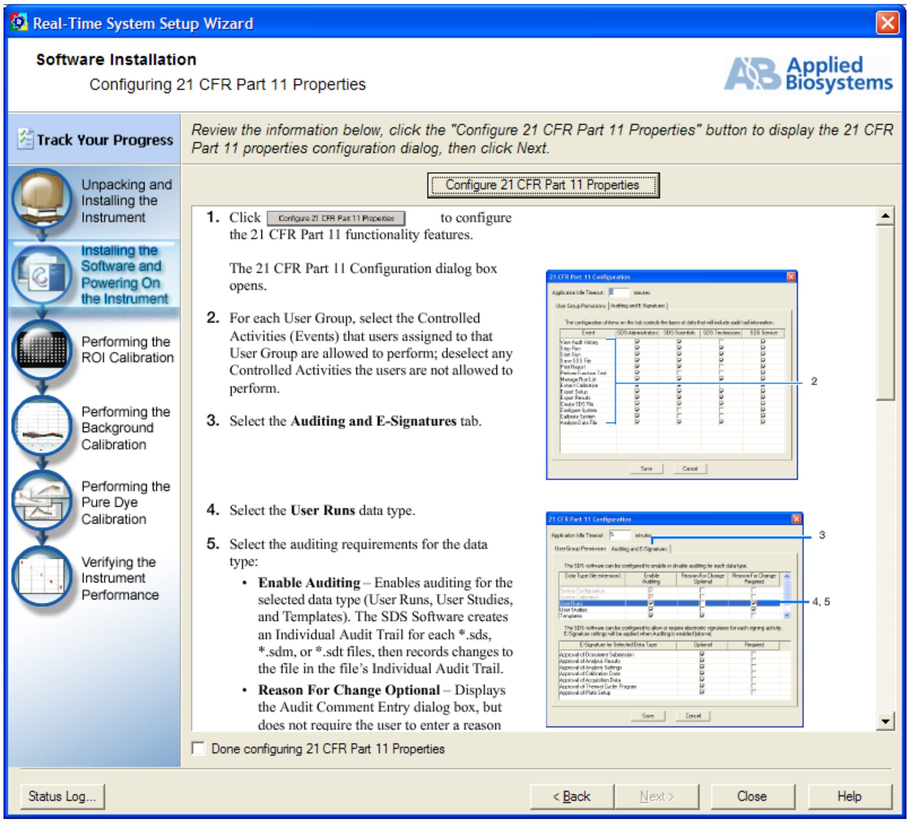
□ Password never expires

□ Account is disabled

□ Done configuring Users and Groups

Notes

c. Configure the 21CFR11 module (**Configure 21 CFR Part 11 Properties** button).



Real-Time System Setup Wizard
Applied Biosystems
Track Your Progress
Unpacking and Installing the Instrument
Installing the Software and Powering On the Instrument
Performing the ROI Calibration
Performing the Background Calibration
Performing the Pure Dye Calibration
Verifying the Instrument Performance
Configure 21 CFR Part 11 Properties
2
3
4, 5
Status Log...
< Back
Next >
Close
Help

Software Installation

Configuring 21 CFR Part 11 Properties

Review the information below, click the "Configure 21 CFR Part 11 Properties" button to display the 21 CFR Part 11 properties configuration dialog, then click Next.

1. Click Configure 21 CFR Part 11 Properties to configure the 21 CFR Part 11 functionality features.

   The 21 CFR Part 11 Configuration dialog box opens.

2. For each User Group, select the Controlled Activities (Events) that users assigned to that User Group are allowed to perform; deselect any Controlled Activities the users are not allowed to perform.

3. Select the **Auditing and E-Signatures** tab.

4. Select the **User Runs** data type.

5. Select the auditing requirements for the data type:
   - **Enable Auditing** – Enables auditing for the selected data type (User Runs, User Studies, and Templates). The SDS Software creates an Individual Audit Trail for each *.sds, *.sdm, or *.sdt files, then records changes to the file in the file's Individual Audit Trail.
   - **Reason For Change Optional** – Displays the Audit Comment Entry dialog box, but does not require the user to enter a reason

□ Done configuring 21 CFR Part 11 Properties

IMPORTANT! When you click the **Configure 21 CFR Part 11 Properties** button, the User Login dialog box appears. During installation, you are required to log in to the SDS Software any time you attempt to perform a Controlled Activity (for example, the *Configure System* and *Perform Function Test* Controlled Activities). For login procedures, see Chapter 3, "Logging in to the SDS Software," on page 23.

5. Complete the installation:
   - If you clicked **Unpack and Set Up a New Instrument** in step 3 on page 9, the wizard provides procedures for performing functional tests and calibration.
   - If you clicked **Install the SDS Software** in step 3 on page 9, the wizard returns to the Welcome screen shown in step 2 on page 9.

Creating User Groups and Configuring After Installation

If necessary, you can also create users and User Groups or configure the 21CFR11 module *after* installation. See the following procedures in this User Guide:

- "Creating Users and User Groups in the Operating System" on page 12
- "Configuring the 21CFR11 Module" on page 31

Notes

Creating Users and User Groups in the Operating System

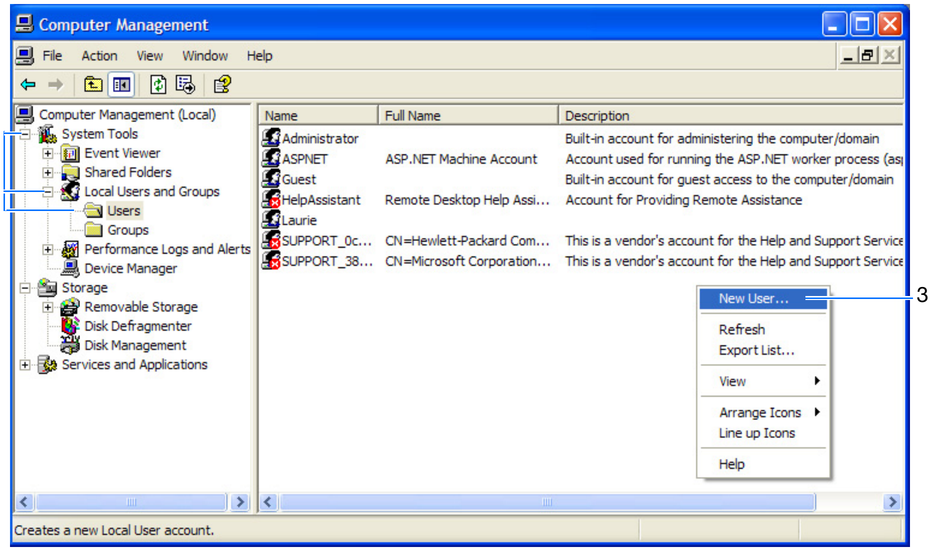
The 21 CFR Part 11 module uses the Microsoft Windows XP operating system to manage user names and passwords. In order for the 21CFR11 module to work correctly, you must create users and User Groups in the Windows XP operating system as described in the procedures below.

Creating Users

IMPORTANT! Be sure to use this procedure when creating users in the Windows XP operating system. Creating a user with the **Start ▸ Control Panel ▸ User Accounts** option does not allow you to enter the user's full name. A user's full name will be needed to record an E-Signature.

1. On your desktop, right-click (**My Computer**), then select **Manage**.

2. In the Computer Management dialog box, select **System Tools ▸ Local Users and Groups ▸ Users**.



Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
ASPNET	ASP.NET Machine Account	Account used for running the ASP.NET worker process (as
Guest		Built-in account for guest access to the computer/domain
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Remote Assistance
Laurie		
SUPPORT_0c...	CN=Hewlett-Packard Com...	This is a vendor's account for the Help and Support Service
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account for the Help and Support Service

Creates a new Local User account.

3. Right-click anywhere in the right-hand panel (where the contents of the Users folder is displayed); in the pop-up menu that appears, click **New User**.

4. Complete the New User dialog box:

   a. In the User name field, type the user's login name (for example, **MSmith**).

   b. In the Full name field, type the user's full name (for example, **Mary Smith**).

   IMPORTANT! The Windows XP operating system allows a blank (empty) Full name field and the SDS Software allows it for all User Groups except the ESignatures User Group. The SDS Software will not allow a user in the ESignatures User Group to record an E-Signature if the user account's Full name field is blank.

Notes

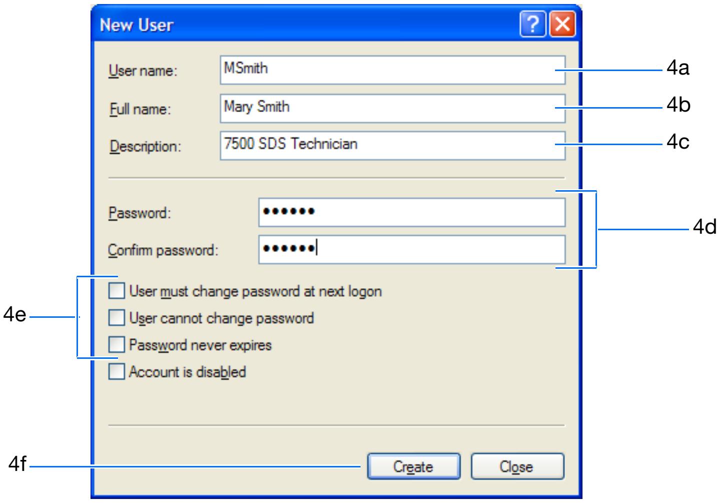
c. (Optional) Type a Description.

d. Type a Password, then retype it to confirm the password.

> **IMPORTANT!** Do not assign blank (empty) passwords. Although the Windows XP operating system accepts blank passwords, the SDS Software does not. Users will receive an error message if they try to log in to the SDS Software without a password.

e. Select the password attributes as desired.

f. Click **Create**.



User name: MSmith

Full name: Mary Smith

Description: 7500 SDS Technician

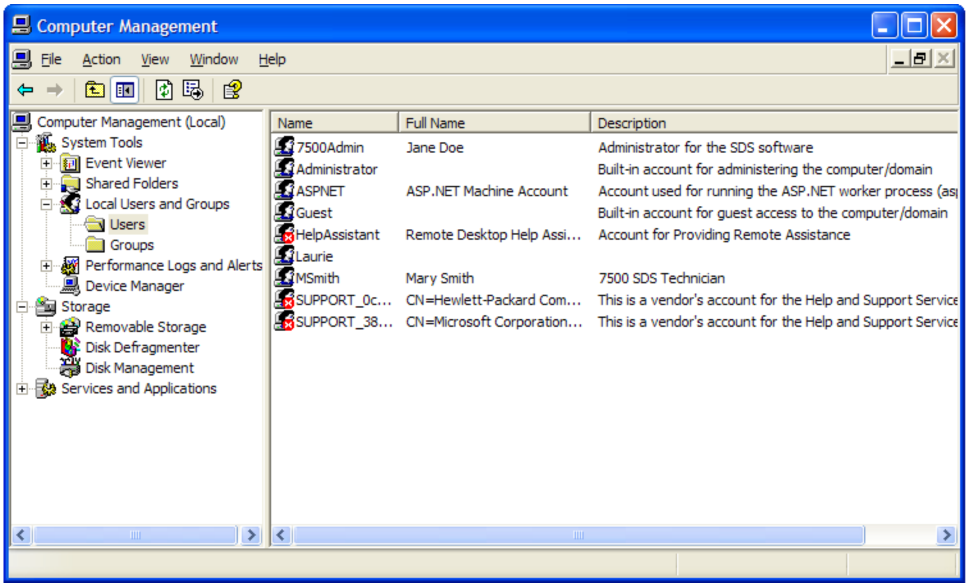
Password: ••••••

Confirm password: ••••••

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled

5. Repeat step 4 for the remaining users.

6. Click **Close** to save the changes and close the New User dialog box. The new users appear in the Computer Management dialog box.



Name	Full Name	Description
7500Admin	Jane Doe	Administrator for the SDS software
Administrator		Built-in account for administering the computer/domain
ASPNET	ASP.NET Machine Account	Account used for running the ASP.NET worker process (as|
Guest		Built-in account for guest access to the computer/domain
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Remote Assistance
Laurie		
MSmith	Mary Smith	7500 SDS Technician
SUPPORT_0c...	CN=Hewlett-Packard Com...	This is a vendor's account for the Help and Support Service
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account for the Help and Support Service

7. Close the Computer Management dialog box.

Creating User Groups

Note: This procedure describes how to create a new User Group, then immediately add users to that group. If you need to add a user to an existing User Group, see page 18.

There are five predefined User Groups in the SDS Software:

- SDS Administrators
- SDS Scientists
- SDS Technicians
- SDS Service
- SDS ESignature

In order for the SDS Software to access these User Groups, you must create the User Groups in the Windows XP operating system, then assign users to each User Group. By assigning a user to a User Group, you can control the user’s ability to perform the Controlled Activities in the SDS Software (see “Configuring User Group Permissions” on page 35).

Note: Users can be assigned to multiple User Groups. Users are allowed to perform any Controlled Activity that is permitted to any of the User Groups to which they are assigned.

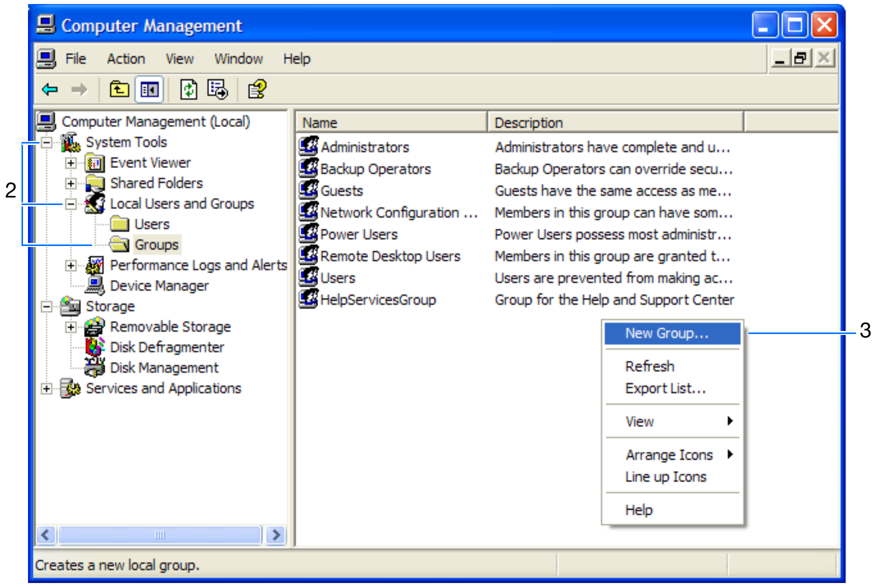
Notes

To create User Groups in the Windows XP operating system:

1. On your desktop, right-click (**My Computer**), then select **Manage**.

2. In the Computer Management dialog box, select **System Tools** ▶ **Local Users and Groups** ▶ **Groups**.

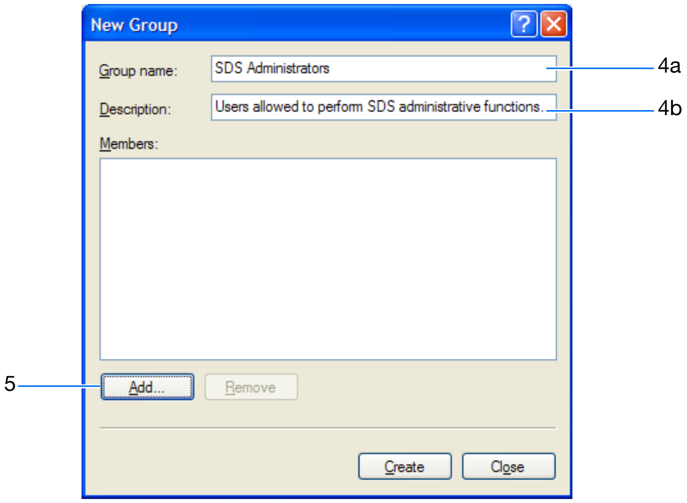
3. Right-click anywhere in the right-hand panel (where the contents of the Groups folder is displayed); in the pop-up menu that appears, click **New Group**.



Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Guests	Guests have the same access as me...
Network Configuration ...	Members in this group can have som...
Power Users	Power Users possess most administr...
Remote Desktop Users	Members in this group are granted t...
Users	Users are prevented from making ac...
HelpServicesGroup	Group for the Help and Support Center

Creates a new local group.

4. Add the SDS Administrators User Group in the New Group dialog box:
   a. In the Group name field, type **SDS Administrators**.
   b. (Optional) Type a Description.



Group name: SDS Administrators

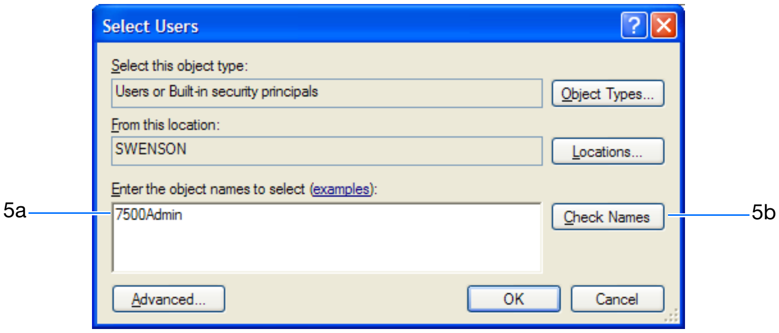
Description: Users allowed to perform SDS administrative functions.

Notes

5. Click **Add** to open the Select Users dialog box.

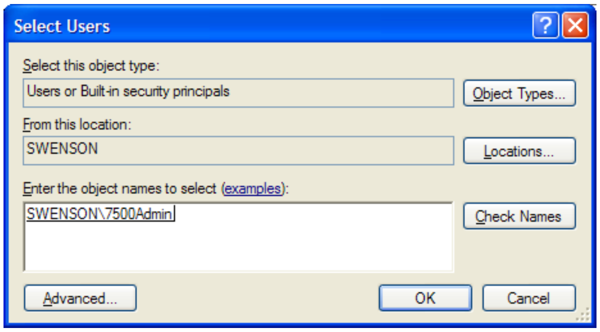
6. Complete the Select Users dialog box:

   a. Type the Windows XP operating system user name of the user you want to add.



Select this object type:
Users or Built-in security principals
From this location:
SWENSON
Enter the object names to select (examples):
7500Admin

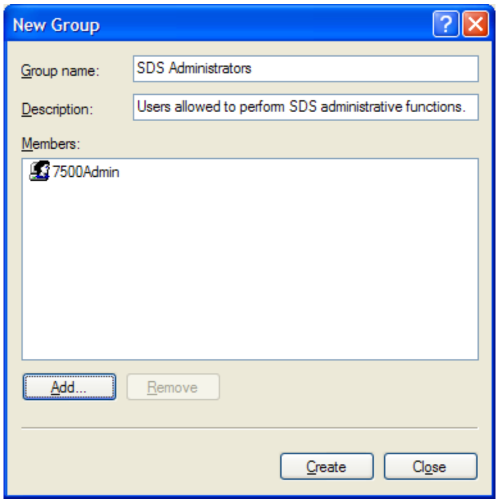
   b. Click **Check Names**. The Select Users dialog box is redisplayed with the user's location and name; verify that you have selected the correct user.



Select this object type:
Users or Built-in security principals
From this location:
SWENSON
Enter the object names to select (examples):
SWENSON\7500Admin

Note: If you have problems locating the correct user, click **Object Types** to be sure the Users checkbox is selected and/or click **Locations** to select the correct location.

   c. Click **OK**. The user name appears in the Members field of the New Group dialog box.



Group name: SDS Administrators

Description: Users allowed to perform SDS administrative functions.

Members: 7500Admin

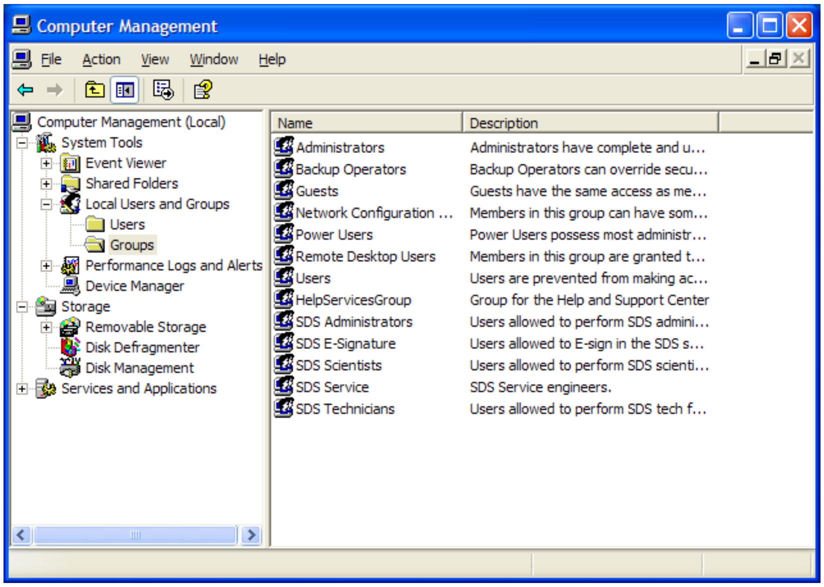
7. Repeat steps 5 and 6 for each user you want to add to the SDS Administrators User Group.

8. Click **Create**. The SDS Administrators User Group is created and the New Group dialog box fields become open (blank).

9. Repeat steps 4 through 8 for the remaining four User Groups:
    - SDS Scientists
    - SDS Technicians
    - SDS Service
    - SDS E-Signature

10. Click **Close** to save the changes and close the New Group dialog box. The five SDS Software User Groups appear in the Computer Management dialog box.

Notes



Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Guests	Guests have the same access as me...
Network Configuration ...	Members in this group can have som...
Power Users	Power Users possess most administr...
Remote Desktop Users	Members in this group are granted t...
Users	Users are prevented from making ac...
HelpServicesGroup	Group for the Help and Support Center
SDS Administrators	Users allowed to perform SDS admini...
SDS E-Signature	Users allowed to E-sign in the SDS s...
SDS Scientists	Users allowed to perform SDS scienti...
SDS Service	SDS Service engineers.
SDS Technicians	Users allowed to perform SDS tech f...

11. Close the Computer Management dialog box.

12. After creating the User Groups, configure the permissions each User Group has to perform the Controlled Activities within the SDS Software. See "Configuring User Group Permissions" on page 35.

Adding a User to an Existing User Group

If you need to add a user to an SDS Software User Group after you have already created the User Group in the Windows XP operating system, follow the procedure below.

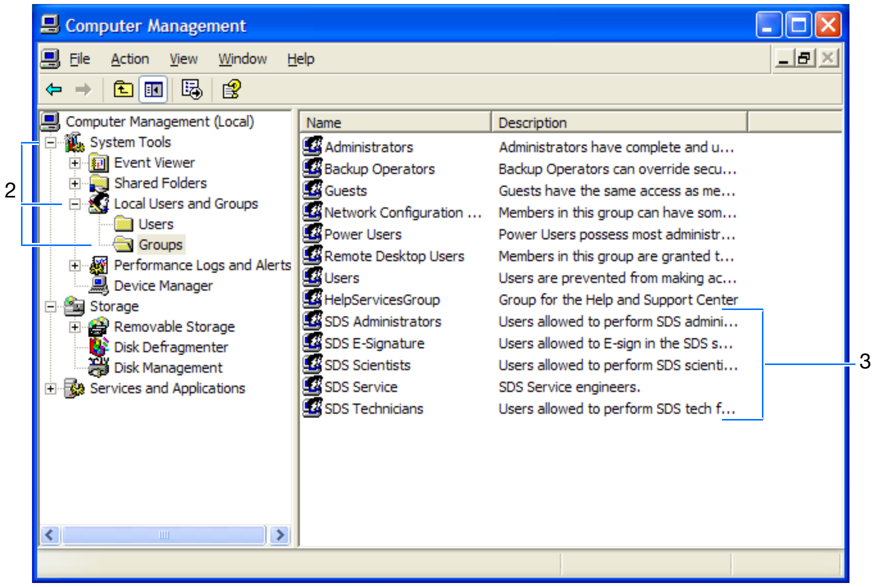
Note: Users can be assigned to multiple User Groups. Users are allowed to perform any Controlled Activity that is permitted to any of the User Groups to which they are assigned.

To add a user to an existing User Group in the Windows XP operating system:

1. On your desktop, right-click (**My Computer**), then select **Manage**.

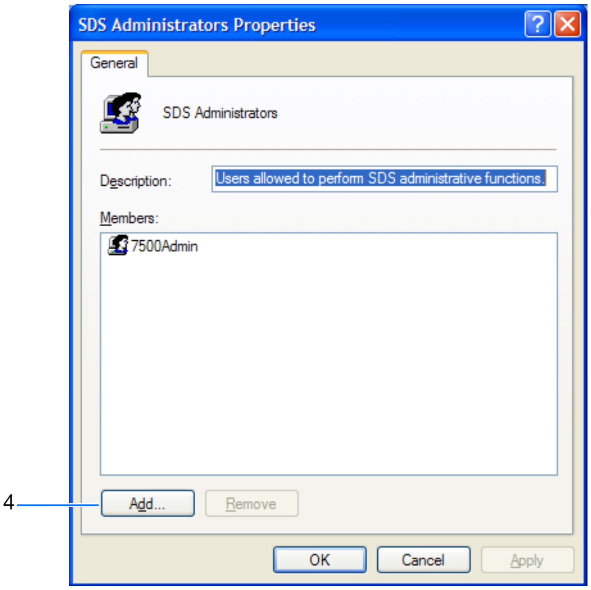
2. In the Computer Management dialog box, select **System Tools** ▸ **Local Users and Groups** ▸ **Groups**.

3. Double-click the appropriate SDS Software User Group.



Name	Description
Administrators	Administrators have complete and u…
Backup Operators	Backup Operators can override secu…
Guests	Guests have the same access as me…
Network Configuration …	Members in this group can have som…
Power Users	Power Users possess most administr…
Remote Desktop Users	Members in this group are granted t…
Users	Users are prevented from making ac…
HelpServicesGroup	Group for the Help and Support Center
SDS Administrators	Users allowed to perform SDS admini…
SDS E-Signature	Users allowed to E-sign in the SDS s…
SDS Scientists	Users allowed to perform SDS scienti…
SDS Service	SDS Service engineers.
SDS Technicians	Users allowed to perform SDS tech f…

4. In the Properties dialog box, click **Add** to open the Select Users dialog box.



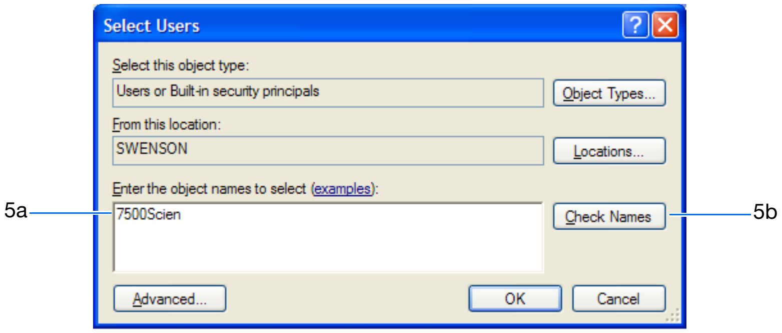
Description: Users allowed to perform SDS administrative functions.

Members:
7500Admin

Notes

5. Complete the Select Users dialog box:

   a. Type the user's Windows XP operating system user name.



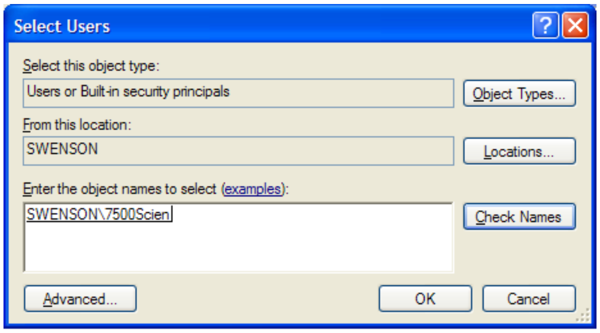
Select Users

Select this object type:
Users or Built-in security principals

From this location:
SWENSON

Enter the object names to select (examples):
7500Scien

   b. Click **Check Names**. The Select Users dialog box is redisplayed with the user's location and name; verify that you have selected the correct user.



Select Users

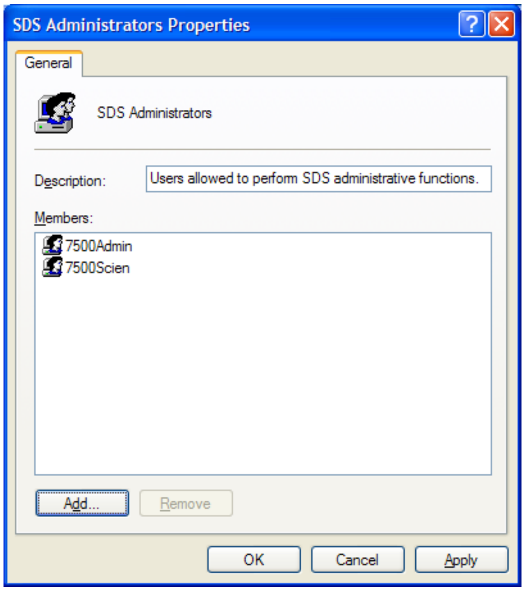
Select this object type:
Users or Built-in security principals

From this location:
SWENSON

Enter the object names to select (examples):
SWENSON\7500Scien

Note: If you have problems locating the correct user, click **Object Types** to be sure the Users checkbox is selected and/or click **Locations** to select the correct location.

   c. Click **OK**. The user name appears in the Members field of the Properties dialog box.



SDS Administrators

Description: Users allowed to perform SDS administrative functions.

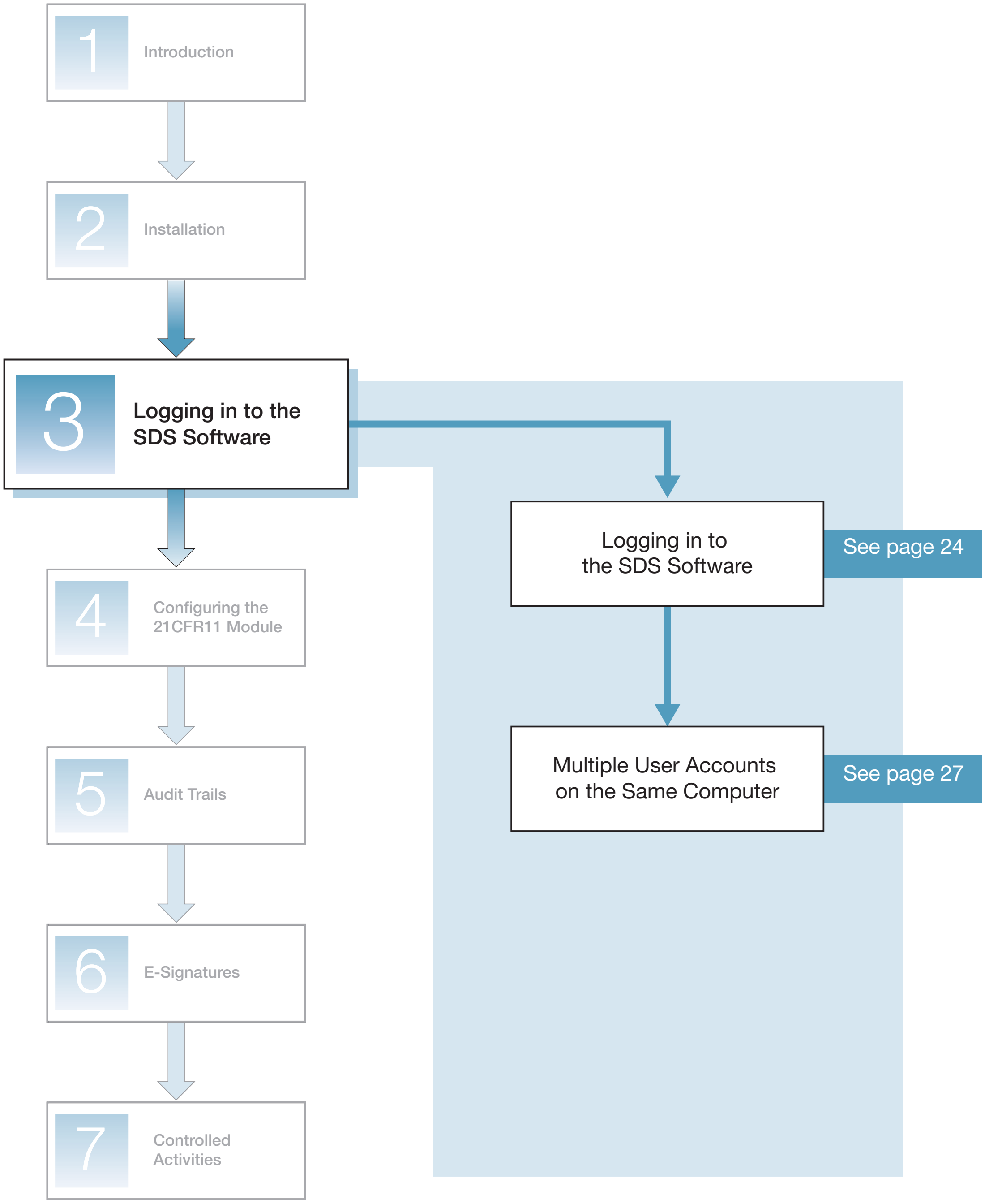
Members:
7500Admin
7500Scien

6. Click **OK** to save the changes and close the Properties dialog box.

7. Close the Computer Management dialog box.

Notes

3 Logging in to the SDS Software


1 Introduction
2 Installation
3 Logging in to the SDS Software
4 Configuring the 21CFR11 Module
5 Audit Trails
6 E-Signatures
7 Controlled Activities
Logging in to the SDS Software
See page 24
Multiple User Accounts on the Same Computer
See page 27

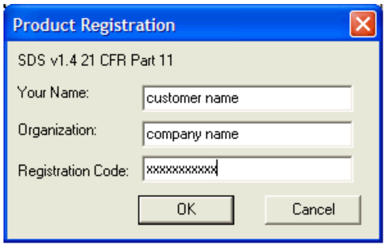
Notes

Logging in to the SDS Software

The 21 CFR Part 11 module requires that users log in to the Sequence Detection Systems Software each time they start the software.

1. Log in to the Microsoft® Windows® XP operating system.
2. On your desktop, double-click (***instrument software***) to start the SDS Software. If you do not have the shortcut on your desktop, select **Start ▸ All Programs ▸ Applied Biosystems ▸ *instrument* ▸ *instrument software***.
3. If the registration code for the 21CFR11 module was not entered at installation, the Product Registration dialog box appears:
   a. Enter your name.
   b. Enter your organization.
   c. Enter the registration code, which can be found on the SDS Software CD case.
   d. Click **OK**.

Note: Once you successfully enter the registration code, the Product Registration dialog box will not be displayed when you log in again.



SDS v1.4 21 CFR Part 11

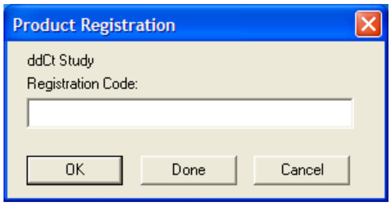
Your Name: customer name

Organization: company name

Registration Code: xxxxxxxxxxx

4. If the registration code for the $\Delta\Delta C_T$ Study was not entered at installation, the Product Registration dialog box appears:
   a. Enter the registration code, which can be found on the SDS Software CD case.
   b. (Optional) Click **OK** to enter additional registration codes.
   c. Click **Done**.

Note: Once you successfully enter the registration code, the Product Registration dialog box will not be displayed when you log in again.



ddCt Study
Registration Code:

5. Complete the User Login dialog box:

   a. **User name** and **Password** – Enter the user name and password for your SDS Software user account. Typically, your SDS Software user name and password are the same as the Windows XP operating system user name and password you entered in step 1 on page 24.

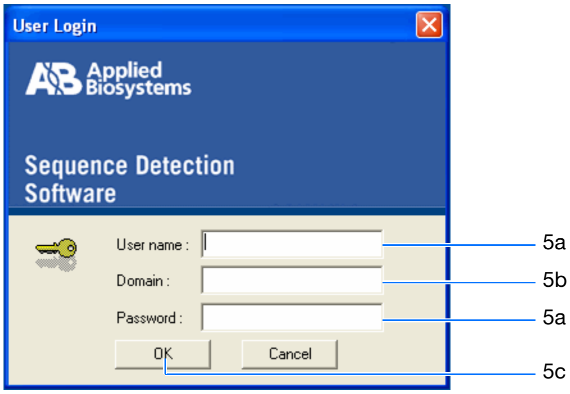
   IMPORTANT! If you have multiple user accounts on the same computer and use different user accounts to log in to the operating system and the SDS Software, see page 27.

   b. (Variable) **Domain** – Enter the name of the domain in which your user account exists. If your user account exists on the local computer, you can enter the local computer's name or leave the Domain field empty.

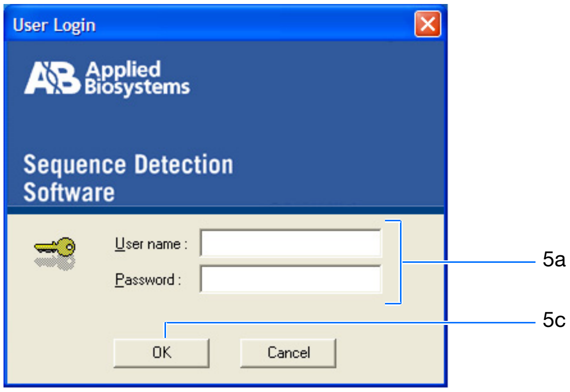
   Note: The Domain field is available if the computer on which you are working is registered in a domain (belongs to a network with domain servers). The Domain field is not available if the computer on which are working is a member of a workgroup (peer-to-peer network or standalone).

   c. Click **OK**. The SDS Software starts.

   Note: If your login information is incorrect, the SDS Software does not start. The failed login attempt is recorded in the Event Log.



User Login dialog box for a computer registered in a domain



User Login dialog box for a computer that is a member of a workgroup

Multiple User Accounts on the Same Computer

User Account Properties

Every user account has:

- A desktop unique from the desktops of all other user accounts.
- Mapped drives that may be different from the mapped drives for other user accounts.
- Access to applications to which other user accounts may not have access (or vice versa).
- Access to drives and directories to which other user accounts may not have access (or vice versa).

Multiple User Accounts

Multiple user accounts can occur on the same computer as follows:

- A single user may have more than one user account on the same computer.
- Several users may be using the same computer.

When multiple user accounts occur on the same computer, the following may be affected:

- Access to the desktop, applications, drives, and directories (below).
- Several functions in the SDS Software (page 28)

Access Scenarios

If there are multiple users accounts on the same computer, the desktop, applications, drives, and directories that are accessible from each user account may be different, as illustrated in the scenarios below.

Scenario	Access From Within the SDS Software	
	Desktop and Applications	**Drives and Directories**
A user logs into the operating system: user name = MSmith. The same user then logs into the SDS Software using the same user account: user name = MSmith.	The user can access the same desktop, applications, drives and directories he or she can access from the operating system.	
A user logs into the operating system: user name = MSmith. The same user then logs into the SDS Software using a different user account: user name = MSmith02.	The user can access the desktop and applications of the account used to log in to the SDS Software. The user may not be able to access the desktop and applications of the account used to log in to the operating system.	The user may or may not be able to access the same drives and directories as in the operating system Explorer, depending on the varying access rights of the two accounts.
A user logs into the operating system: user name = MSmith. A second user then logs into the SDS Software: user name = JDoe.		

Notes

Affected Functions

If a user is logged in to the SDS Software with a different user account than the user account logged in to the Windows XP operating system, the user may encounter errors when performing the following functions in the SDS Software:

- File ▸ Open
- File ▸ Save
- File ▸ Save As
- File ▸ Import Sample Setup
- File ▸ Export ▸ Sample Setup
- File ▸ Export ▸ Calibration Data
- File ▸ Export ▸ Spectra
- File ▸ Export ▸ Component
- File ▸ Export ▸ Rn
- File ▸ Export ▸ Delta Rn
- File ▸ Export ▸ Ct
- File ▸ Export ▸ Dissociation ▸ Raw & Derivative Data
- File ▸ Export ▸ Dissociation ▸ Tm
- File ▸ Export ▸ Results
- File ▸ View Exported Results
- File ▸ Print
- Export as JPEG
- Export To PowerPoint
- Export All To PowerPoint

Preventing Errors

Be sure your user account(s) is configured in the Windows XP operating system to have:

- Read/write access to the desired directories
- Create access in the desired directories
- Access to the desired printers
- Access to the Microsoft® PowerPoint® Software

Note: The PowerPoint Software must be installed on the computer.

For directory and printer access, see your SDS Software System Administrator or the Windows XP operating system documentation.

For PowerPoint Software access:

1. Log in to the Windows XP operating system with the user account causing the error in the SDS Software.

2. Select **Start** ▸ **All Programs** ▸ **Microsoft PowerPoint**.

Notes

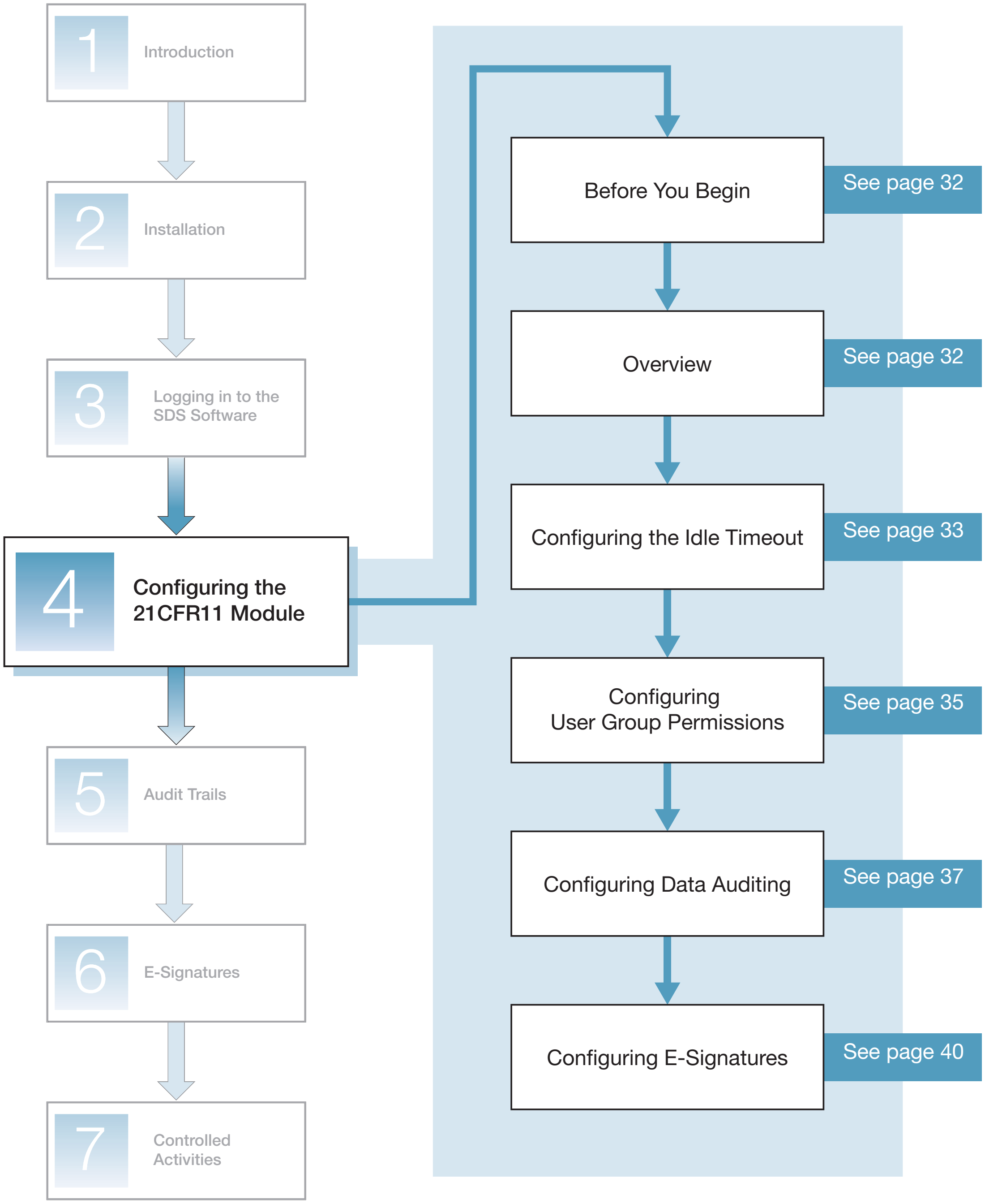
3. At the prompt, click **OK** to run the installation program.

IMPORTANT! You must repeat this procedure for *each* user account that will perform the Export To PowerPoint and Export All To PowerPoint functions in the SDS Software.

Notes

Notes

4 Configuring the 21CFR11 Module



Notes

Before You Begin

User Group Permissions

To perform the procedures in this chapter, you must:

- Log in to the SDS Software as a member of a User Group that has permission to perform the *Configure System* Controlled Activity. (For information on configuring User Group Permissions, see page 35. For information on Controlled Activities, see Chapter 7 on page 71.)

  Or
- Be a member of the Administrators group in the Microsoft® Windows® XP operating system and log in to the SDS Software with a valid SDS Software user account.

Note: As a cautionary measure, any user who is a member of the Administrators group in the Windows XP operating system is always allowed to open the configuration utility (Config21cfr11.exe) and configure the 21CFR11 module.

Logging In

For login procedures, see Chapter 3 on page 23.

Overview

Configurable Features

You can tailor the following features of the 21CFR11 module to support your company's Standard Operating Procedures (SOPs) and controls:

- **Idle timeout** – The amount of time a user can remain inactive (no mouse or keyboard activity) before the SDS Software automatically logs the user out (page 33).
- **User Group Permissions** – The authorization each User Group has to perform predefined Controlled Activities (page 35).
- **Data auditing** – The File Types that maintain audit trails, when to prompt for an audit trail comment, and whether a comment entry is optional or required (page 37).
- **E-Signatures** – The File Types that maintain E-Signatures and whether an E-Signature is optional or required for predefined Signing Types (page 40).

Auditing of System Configuration Data

Any saved changes you make to the 21CFR11 module are audited. Configuring the 21CFR11 module falls under the *System Configuration* File Type category. For this File Type:

- Auditing is always enabled.
- The auditing is silent (that is, a Reason for Change Entry dialog box is never displayed).

Notes

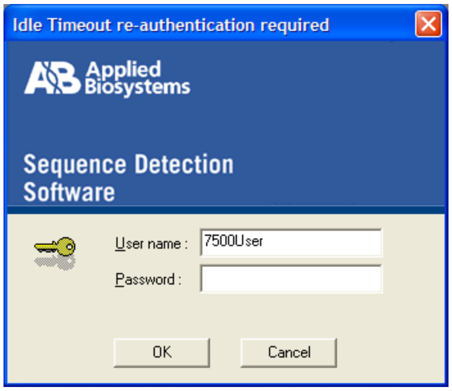
- All saved changes are recorded in the Configuration Audit Trail.

Note: For information on auditing of File Types, see "File Types" on page 37. For information on the Configuration Audit Trail, see "Viewing the Configuration Audit Trail" on page 49.

Configuring the Idle Timeout

You can set the amount of time a user can remain inactive before the SDS Software automatically logs the user out.

If a user is logged in and is inactive (no mouse or keyboard activity) for the configured Idle Timeout period, the SDS Software automatically logs the user out and displays the Idle Timeout dialog box shown below. A user cannot perform any activities in the SDS Software until he or she successfully logs in.


Idle Timeout re-authentication required
Applied Biosystems
Sequence Detection Software
OK
Cancel

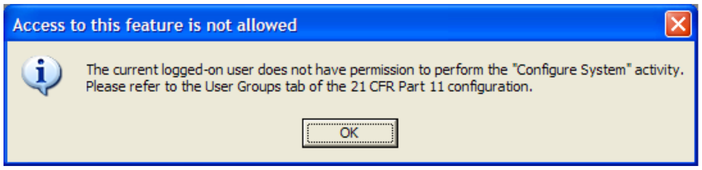
User name : 7500User

Password :

Note: The Idle Timeout dialog box may also include the Domain field. For more information, see "Logging in to the SDS Software" on page 24.

Setting the Idle Timeout

1. In the SDS Software main menu, select **21CFR11 ▸ Configuration (Admin Only)**. If you do not have permission to perform the *Configure System* Controlled Activity, the alert message below is displayed.

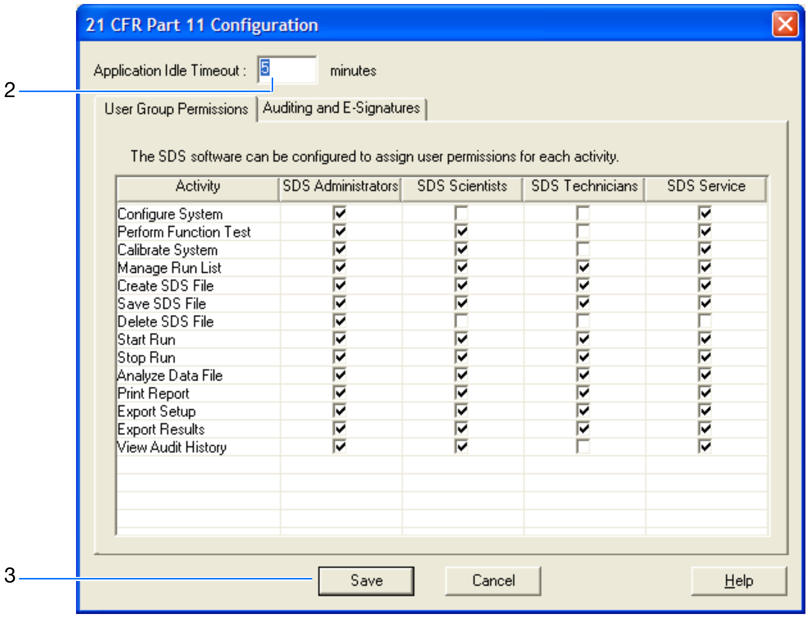


The current logged-on user does not have permission to perform the "Configure System" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Notes

2. In the Application Idle Timeout field, type the desired value. You can enter any value from **0** to **600** minutes.

IMPORTANT! If you enter **0** minutes, the SDS Software will never timeout.



Application Idle Timeout : 5 minutes

The SDS software can be configured to assign user permissions for each activity.

Activity	SDS Administrators	SDS Scientists	SDS Technicians	SDS Service
Configure System	☑	□	□	☑
Perform Function Test	☑	☑	□	☑
Calibrate System	☑	☑	□	☑
Manage Run List	☑	☑	☑	☑
Create SDS File	☑	☑	☑	☑
Save SDS File	☑	☑	☑	☑
Delete SDS File	☑	□	□	□
Start Run	☑	☑	☑	☑
Stop Run	☑	☑	☑	☑
Analyze Data File	☑	☑	☑	☑
Print Report	☑	☑	☑	☑
Export Setup	☑	☑	☑	☑
Export Results	☑	☑	☑	☑
View Audit History	☑	☑	□	☑

3. Click **Save**. The SDS Software saves the changes. The changes are recorded in the Configuration Audit Trail.

Configuring User Group Permissions

Controlled Activities

Controlled Activities are operations within the SDS Software that users can either be allowed to perform or prevented from performing. The following Controlled Activities are predefined in the SDS Software:

Controlled Activity	When selected‡ in the User Group Permissions tab, allows the User Group members to...
Analyze Data File	Analyze runs for *.sds files.
Calibrate System	Calibrate the Real-Time PCR System.
Configure System	Configure the SDS Software 21CFR11 module.
Create SDS File	Create *.sds, *.sdm, or *.sdt files.
Delete SDS File	Delete *.sds, *.sdm, or *.sdt files.
Export Results	Export results for *.sds, *.sdm, or *.sdt files.
Export Setup	Export setup information for *.sds or *.sdt files.
Manage Run List	Access the Run List Manager, where *.sds or *.sdm files can be opened, moved, deleted, or imported.
Perform Function Test	Perform the Real-Time PCR System functional tests.
Print Report	Print reports for *.sds, *.sdm, and *.sdt files.
Save SDS File	Save *.sds, *.sdm, or *.sdt files.
Start Run	Start runs for *.sds files.
Stop Run	Stop runs for *.sds files.
View Audit History	View the audit trails. (For more information, see "Viewing Audit Trails" on page 49.)

‡ When the Controlled Activity is deselected in the User Group Permissions tab, the User Group members are prevented from performing the activity.

User Groups

You can assign permissions to perform the Controlled Activities to the following User Groups:

- SDS Administrators
- SDS Scientists
- SDS Technicians
- SDS Service

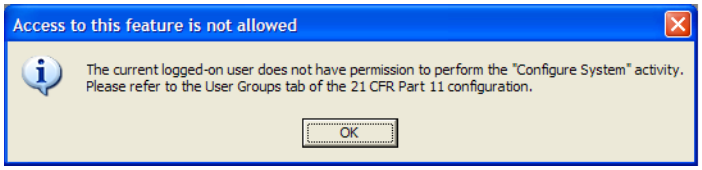
Note: You cannot assign permissions to perform any of the Controlled Activities to the SDS ESignature User Group. The ESignature User Group is only used to define the set of users who are allowed to sign data (record E-Signatures). For more information, see "Configuring E-Signatures" on page 40.

Notes

4

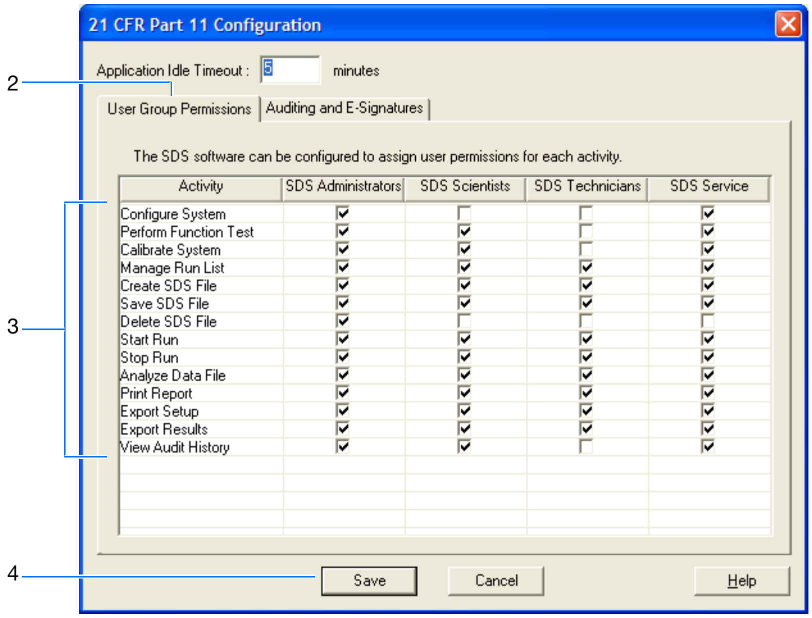
Configuring User Group Permissions

1. In the SDS Software main menu, select **21CFR11 ▶ Configuration (Admin Only)**. If you do not have permission to perform the *Configure System* Controlled Activity, the alert message below is displayed.



The current logged-on user does not have permission to perform the "Configure System" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

2. Select the **User Group Permissions** tab (default).



Application Idle Timeout : 5 minutes

The SDS software can be configured to assign user permissions for each activity.

Activity	SDS Administrators	SDS Scientists	SDS Technicians	SDS Service
Configure System	☑	□	□	☑
Perform Function Test	☑	☑	□	☑
Calibrate System	☑	☑	□	☑
Manage Run List	☑	☑	☑	☑
Create SDS File	☑	☑	☑	☑
Save SDS File	☑	☑	☑	☑
Delete SDS File	☑	□	□	□
Start Run	☑	☑	☑	☑
Stop Run	☑	☑	☑	☑
Analyze Data File	☑	☑	☑	☑
Print Report	☑	☑	☑	☑
Export Setup	☑	☑	☑	☑
Export Results	☑	☑	☑	☑
View Audit History	☑	☑	□	☑

3. For each User Group, select the Controlled Activities that users assigned to that User Group are allowed to perform; deselect any Controlled Activities the users are not allowed to perform.

4. Click **Save**. The SDS Software saves the changes. The changes are recorded in the Configuration Audit Trail.

Notes

Configuring Data Auditing

Note: This section describes how to configure data auditing. For information on recording and viewing audit trails, see Chapter 5 on page 45.

File Types

The File Types discussed in this document can be configured for data auditing as described in the table below.

File Type	Configurable	Audit Trail
User Runs	Yes. You can configure these File Types for data auditing. Additionally, you can configure a user comment (Reason For Change) to be optional or required.	If data auditing is enabled, transactions are recorded in an Individual Audit Trail for the *.sds, *.sdm, or *.sdt file.
User Studies		
Templates		
System Configuration	No. You cannot configure these File Types for data auditing. These File Types are always audited and the auditing is silent (that is, a Reason for Change Entry dialog box is never displayed to users).	Transactions are recorded in the Configuration Audit Trail.
System Calibration		Transactions are recorded in the Calibration Audit Trail.
System Run List		Transactions are recorded in the Run List Audit Trail.

Individual Audit Trails

When data auditing is enabled for the User Runs, User Studies, or Templates File Types, the SDS Software creates an Individual Audit Trail for each *.sds, *.sdm, or *.sdt file. When a user saves changes (creations, deletions, or updates) to a file, the SDS Software records the following information in the Individual Audit Trail:

- **Date & Time** – The date and time the change occurred.
- **User Login** – The name on the logged-in user account when the change occurred. The user account's login name is recorded here, rather than the full name.
- **Changed Data** – The type of data that was affected by the change.
- **Reason for Change** – Any text the user may have entered in the text field of the Reason for Change Entry dialog box when making the change.
- **Details/Previous Value** – The previous value of the changed data.

IMPORTANT! Changes to an *.sds, *.sdm, or *.sdt file are only recorded in the file's Individual Audit Trail when the changes are saved by a user. Changes are not recorded in the Individual Audit Trail as fields are modified. For example, if a user changes the Sample Volume field in an *.sds file from 50 to 40 to 30 to 10, then saves the *.sds file, only one entry–indicating the changed volume from 50 to 10–is recorded in the file's Individual Audit Trail.

Notes

Individual Audit Trails for User Studies

For *.sdm files, the Individual Audit Trail maintains the history for the User Study itself. As *.sds files are added to the User Study, the SDS Software creates an embedded copy of the added *.sds file into the User Study; the User Study then has a snapshot of the *.sds file's Individual Audit Trail. If the *.sds file is subsequently updated, the additional entries to the *.sds file's Individual Audit Trail are not part of and do not affect the User Study's Individual Audit Trail.

Configuration, Calibration, and Run List Audit Trails

Data auditing is always enabled for the System Configuration, System Calibration, and System Run List File Types. When a user makes changes (creations, deletions, or updates) to these System files, the SDS Software records the information below in the appropriate audit trail.

Configuration and Calibration Audit Trails

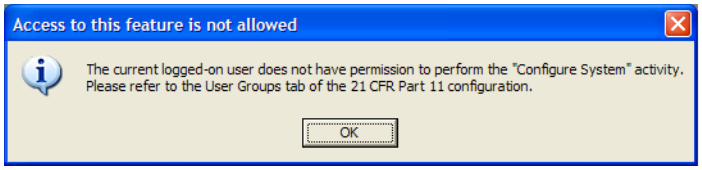
- **Date & Time** – The date and time the change occurred.
- **User Login** – The name on the logged-in user account when the change occurred. The user account's login name is recorded here, rather than the full name.
- **Changed Data** – The type of data that was affected by the change.
- **Reason for Change** – This field is empty (blank).
- **Details/Previous Value** – The previous value of the changed data.

Run List Audit Trail

- **Date & Time** – The date and time the event occurred.
- **User Login** – The name on the logged-in user account when the event occurred. The user account's login name is recorded here, rather than the full name.
- **Event** – The event that occurred: *Failed E-Signature*, *Failed Login,* or *Successful Login*.

Configuring Data Auditing

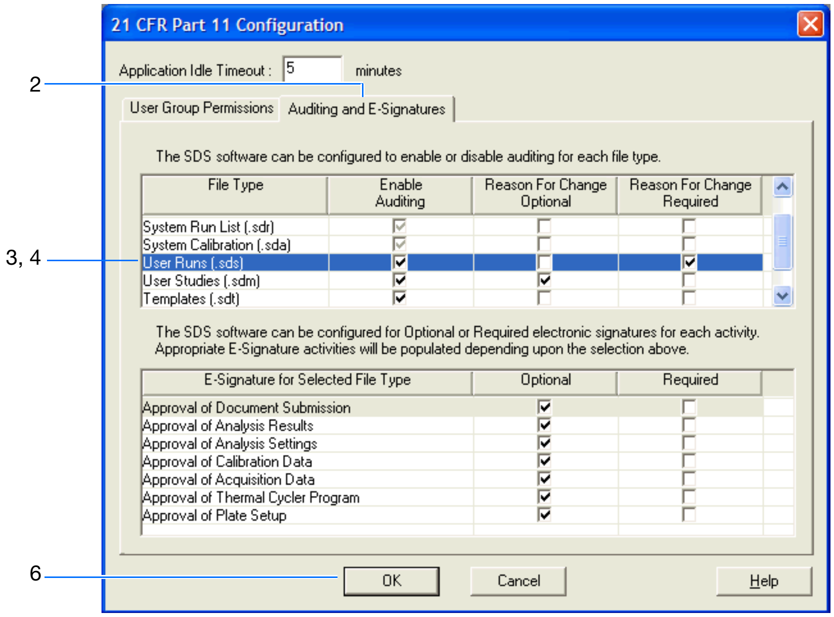
1. In the SDS Software main menu, select **21CFR11 ▸ Configuration (Admin Only)**. If you do not have permission to perform the *Configure System* Controlled Activity, the alert message below is displayed.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Configure System" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

2. Select the **Auditing and E-Signatures** tab.



21 CFR Part 11 Configuration

Application Idle Timeout : 5 minutes

User Group Permissions | Auditing and E-Signatures

The SDS software can be configured to enable or disable auditing for each file type.

File Type	Enable Auditing	Reason For Change Optional	Reason For Change Required
System Run List (.sdr)	☑	□	□
System Calibration (.sda)	☑	□	□
User Runs (.sds)	☑	□	☑
User Studies (.sdm)	☑	☑	□
Templates (.sdt)	☑	□	□

The SDS software can be configured for Optional or Required electronic signatures for each activity. Appropriate E-Signature activities will be populated depending upon the selection above.

E-Signature for Selected File Type	Optional	Required
Approval of Document Submission	☑	□
Approval of Analysis Results	☑	□
Approval of Analysis Settings	☑	□
Approval of Calibration Data	☑	□
Approval of Acquisition Data	☑	□
Approval of Thermal Cycler Program	☑	□
Approval of Plate Setup	☑	□

3. Select the **User Runs** File Type (default).

4. Select the desired auditing requirements for the File Type:
   - **Enable Auditing** – Enables auditing for the selected File Type (User Runs, User Studies, and Templates). The SDS Software creates an Individual Audit Trail for each *.sds, *.sdm, or *.sdt file, then records changes to the file in the file's Individual Audit Trail.
   - **Reason For Change Optional** – Displays the Reason for Change Entry dialog box, but does not require the user to enter a reason for the change in the text field. If the user does not enter a reason, the SDS Software proceeds.
   - **Reason For Change Required** – Displays the Reason for Change Entry dialog box and requires the user to enter a reason for the change in the text field. If the user does not enter a reason, the SDS Software does not proceed.

IMPORTANT! If you select **Enable Auditing** for a File Type, but do not select either **Reason For Change Optional** or **Reason For Change Required**, the auditing is silent for that File Type (that is, a Reason for Change Entry dialog box is never displayed to users). Additionally, the Signing Type will not appear in the Reason drop-down list of the Electronic Signature dialog box.

5. Repeat steps 3 and 4 for the remaining File Types:
   - **User Studies**
   - **Templates**

Note: You cannot configure the System Configuration, System Calibration, or System Run List File Types for data auditing.

Notes

6. Click **Save**. The SDS Software saves the changes. The changes are recorded in the Configuration Audit Trail.

Configuring E-Signatures

Note: This section describes how to configure E-Signatures. For information on recording and viewing E-Signatures, see Chapter 6 on page 57.

File Types

The File Types discussed in this document can be configured for E-Signatures as described in the table below.

File Type	Configurable	E-Signature Tab
User Runs	Yes. You can configure these File Types to record E-Signatures for predefined Signing Types. Additionally, you can configure the E-Signature to be optional or required for each Signing Type.	E-Signatures are recorded in the E-Signatures tab in each *.sds, *.sdm, or *.sdt file.
User Studies		
Templates		
System Calibration		E-Signatures are recorded in the Calibration E-Signatures tab in the Instrument window.
System Configuration	No. You cannot configure these File Types to record E-Signatures as there are no predefined Signing Types.	NA
System Run List		

Data Auditing and E-Signatures

Data auditing must be enabled for a File Type in order to record E-Signatures for that File Type. For example, if you want E-Signatures to be recorded for the User Runs File Type, you must enable data auditing for User Runs.

If you do not manually enable data auditing for the File Type (page 37), the SDS Software automatically does it for you when you select the E-Signature requirements for a Signing Type (see step 4 on page 42).

Signing Types

For each File Type, E-Signatures can be recorded for the Signing Types predefined in the SDS Software, as listed in the table below.

Note: For a description of each Signing Type, see "Signing Types" on page 58.

File Type‡	Signing Type
System Calibration	Approval of Document Submission
	Approval of Calibration Data

File Type‡	Signing Type
User Runs	Approval of Document Submission
	Approval of Analysis Results
	Approval of Analysis Settings
	Approval of Calibration Data
	Approval of Acquisition Data
	Approval of Thermal Cycler Program
	Approval of Plate Setup
User Studies	Approval of Document Submission
	Approval of Analysis Results
	Approval of Analysis Settings
Templates	Approval of Document Submission
	Approval of Thermal Cycler Program
	Approval of Plate Setup

‡ There are no predefined Signing Types for the *System Configuration* or *System Run List* File Types.

E-Signatures Tabs

For the System Calibration File Type, the SDS Software records E-Signatures in the Calibration E-Signatures tab in the Instrument window. For the User Runs, User Studies, and Templates File Types, the SDS Software records E-Signatures in the E-Signatures tab in each *.sds, *.sdm, or *.sdt file. The SDS Software records the following information in the E-Signatures tabs:

- **Date & Time** – The date and time the E-Signature was recorded.
- **User Printed Name** – The name on the logged-in user account when the E-Signature was recorded. The user account's full name is recorded here, rather than the login name.
- **Signed Data** – The Signing Type for which the E-Signature was recorded.
- **Status** – The status of the data for which the E-Signature was recorded.
- **Comment** – Any text the user may have entered in the Comment field of the Electronic Signatures dialog box.
- **E-Signed Data pane** – Displays the details of the signed data.

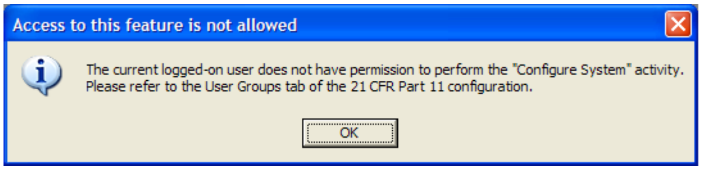
SDS ESignature User Group

Only users who are members of the SDS ESignature User Group are allowed to electronically sign data. For information on assigning users to the SDS ESignature User Group, see "Creating Users and User Groups in the Operating System" on page 12.

IMPORTANT! Applied Biosystems recommends that your company provides additional controls and SOPs for qualified E-Signature users.

Configuring E-Signatures

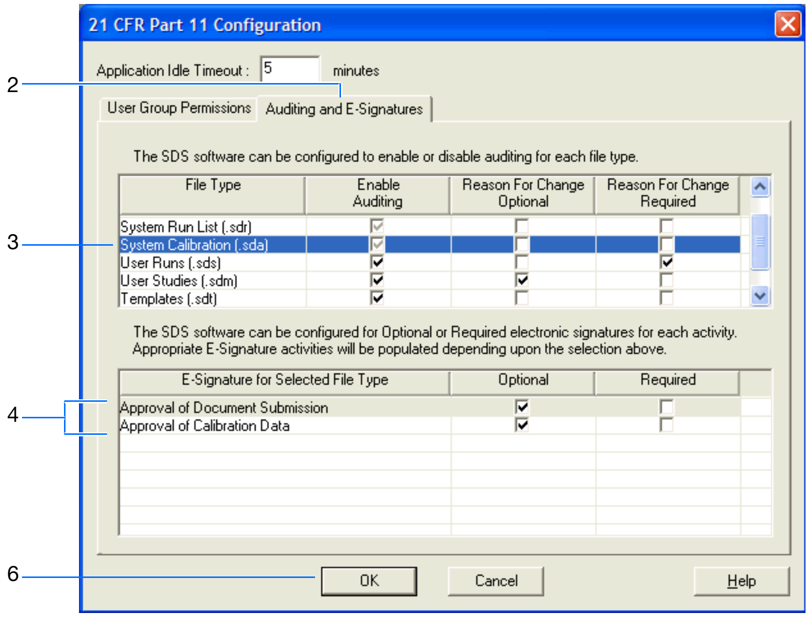
1. In the SDS Software main menu, select **21CFR11 ▸ Configuration (Admin Only)**. If you do not have permission to perform the *Configure System* Controlled Activity, the alert message below is displayed.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Configure System" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

2. Select the **Auditing and E-Signatures** tab.



21 CFR Part 11 Configuration

Application Idle Timeout : 5 minutes

User Group Permissions | Auditing and E-Signatures

The SDS software can be configured to enable or disable auditing for each file type.

File Type	Enable Auditing	Reason For Change Optional	Reason For Change Required
System Run List (.sdr)	☑	□	□
System Calibration (.sda)	☑	□	□
User Runs (.sds)	☑	□	☑
User Studies (.sdm)	☑	☑	□
Templates (.sdt)	☑	□	□

The SDS software can be configured for Optional or Required electronic signatures for each activity. Appropriate E-Signature activities will be populated depending upon the selection above.

E-Signature for Selected File Type	Optional	Required
Approval of Document Submission	☑	□
Approval of Calibration Data	☑	□

3. Select the **System Calibration** File Type.

4. Select the desired E-Signature requirement for each Signing Type specified for the File Type:
   - **Optional** – A user in the ESignature User Group can electronically sign for the selected Signing Type (for example, *Approval of Document Submission*).
   - **Required** – A user in the ESignature User Group must electronically sign for the selected Signing Type. If an E-Signature is not recorded, the SDS Software restricts further action(s) related to the Signing Type. For more information, see "Restrictions for Required E-Signatures" on page 61.

Note: If you have not manually enabled data auditing for the File Type (page 37), the SDS Software automatically does it for you when you select **Optional** or **Required** for the Signing Type.

Notes

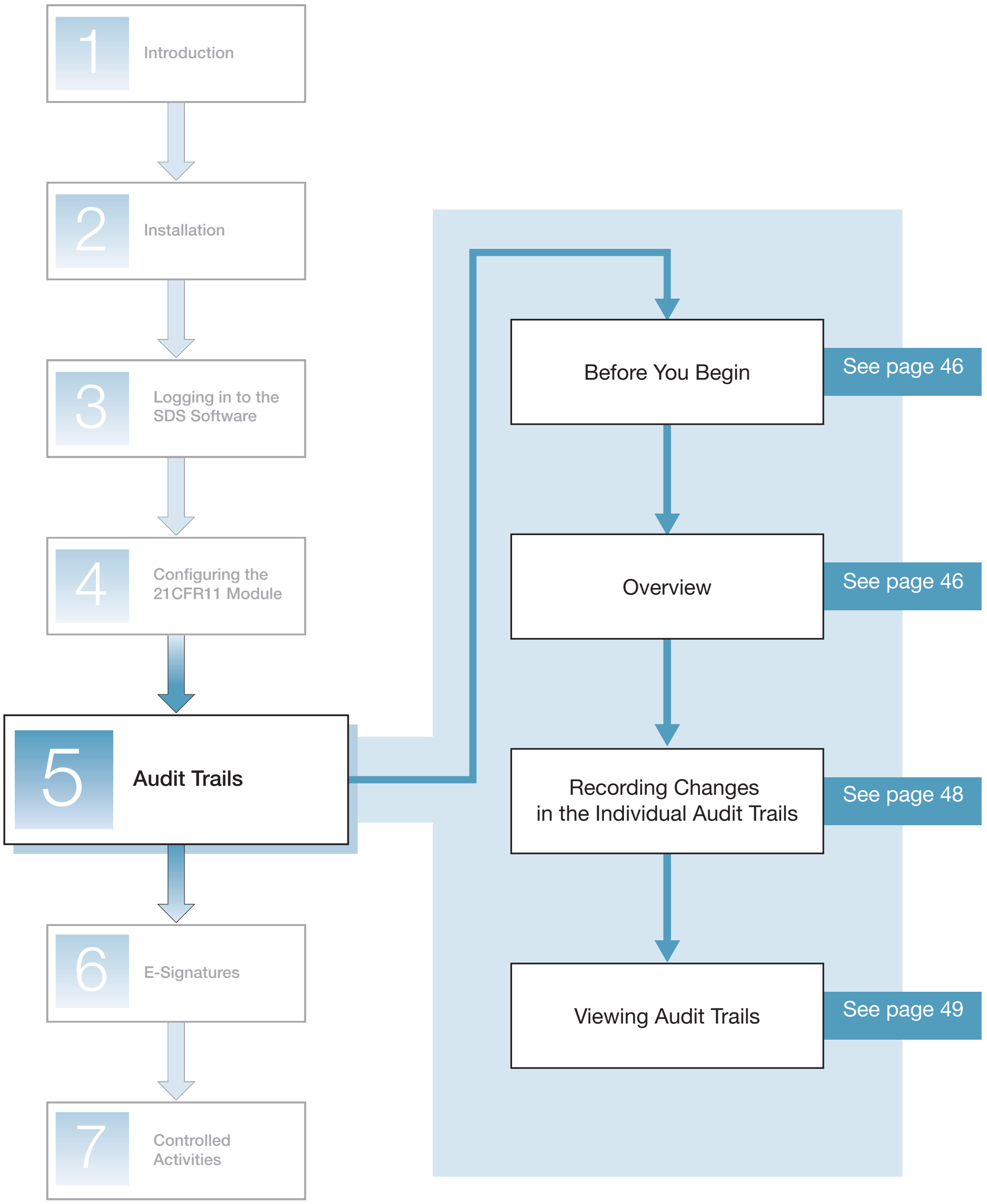
5. Repeat steps 3 and 4 for the remaining File Types:
   - **User Runs**
   - **User Studies**
   - **Templates**

   Note: You cannot configure the System Configuration or System Run List File Types to record E-Signatures as there are no predefined Signing Types.

6. Click **Save**. The SDS Software saves the changes. The changes are recorded in the Configuration Audit Trail.

Notes

5 Audit Trails



Notes

Before You Begin

User Group Permissions

To perform the procedures in this chapter, you must log in to the SDS Software as a member of the User Group specified in each procedure. For information on configuring User Group Permissions, see page 35.

Logging In

For login procedures, see Chapter 3 on page 23.

Overview

Audit Trails

Audit trails are electronic records of transactions that occur within the SDS Software. There are four audit trail types within the SDS Software:

Name	Description
Configuration Audit Trail	Displays the history of creations, deletions, or updates that occur in system configuration data. This includes configuration data for the 21CFR11 module, system analysis parameters, and hardware.
Calibration Audit Trail	Displays the history of creations, deletions, or updates that occur in system calibration data collected from a 7500/7500 Fast instrument. **Note:** Each 7500/7500 Fast instrument generates its own calibration data. Each instrument's calibration data should be applied only to assays performed on that instrument.
Individual Audit Trail	Displays the history of creations, deletions, or updates that occur in an *.sds, *.sdm, or *.sdt file.
Run List Audit Trail	Displays the history of creations, deletions, or updates of the *.sds or *.sdm files that are included in the System Run List.

Event Log

The SDS Software also maintains an Event Log, which displays the history of System Audit Events that occur in the system files. There are three predefined System Audit Events:

- Failed login attempt
- Successful login
- Failed E-Signature attempt

Data Auditing Configuration

System Calibration, System Configuration, and System Run List

For the System Calibration, System Configuration, and System Run List File Types:

- Data auditing is always enabled.
- The auditing is silent (that is, a Reason for Change Entry dialog box is never displayed to users).

Notes

- All saved changes are recorded in the appropriate audit trail:
  - Configuration Audit Trail
  - Calibration Audit Trail
  - Run List Audit Trail

  Transactions are recorded for the life of the Real-Time PCR System.

User Runs, User Studies, and Templates

For the User Runs, User Studies, and Templates File Types, auditing can be configured by the SDS Software System Administrator as described in the table below.

Configuration	Description	Audit Trail
Enabled and silent	Saved changes are recorded when a user creates, deletes, or updates the file. A Reason for Change Entry dialog box is never displayed.	All saved changes are recorded in the file’s Individual Audit Trail. Transactions are recorded for the life of the file.
Enabled, with Reason For Change Optional	Saved changes are recorded when a user creates, deletes, or updates the file. A Reason for Change Entry dialog box is displayed and the user may optionally enter a reason for the change.	
Enabled, with Reason For Change Required	Saved changes are recorded when a user creates, deletes, or updates the file. A Reason for Change Entry dialog box is displayed and the user must enter a reason for the change.	
Disabled	Saved changes are not recorded. A Reason for Change Entry dialog box is never displayed.	An Individual Audit Trail is not maintained for the file.

IMPORTANT! The SDS Software does not maintain Individual Audit Trails for legacy files (*.sds, *.sdm, or *.sdt files from an earlier version of the SDS Software), even when data auditing is enabled for the File Type.

IMPORTANT! Changes to an *.sds, *.sdm, or *.sdt file are only recorded in the file’s Individual Audit Trail when the changes are saved by a user. Changes are not recorded in the Individual Audit Trail as fields are modified. For example, if a user changes the Sample Volume field in an *.sds file from 50 to 40 to 30 to 10, then saves the *.sds file, only one entry–indicating the changed volume from 50 to 10–is recorded in the file’s Individual Audit Trail.

Note: For information on configuring data auditing, see page 37.

Using the Save As Function

When using the Save As function for *.sds, *.sdm, or *.sdt files, be aware of the following data auditing issues:

- The original file remains unchanged.

- The new file is enabled/disabled for data auditing per the current data auditing configuration for the File Type (User Runs, User Studies, or Templates).
- If the original file contains an Individual Audit Trail and data auditing is currently enabled for the File Type, the original file's Individual Audit Trail is copied to the new file. In the new file's Individual Audit Trail, the Event column displays *Created From File* and the Data column displays the original file's name.
- If the original file contains E-Signatures and data auditing is currently enabled for the File Type, the original file's E-Signatures are copied to the new file.

Recording Changes in the Individual Audit Trails

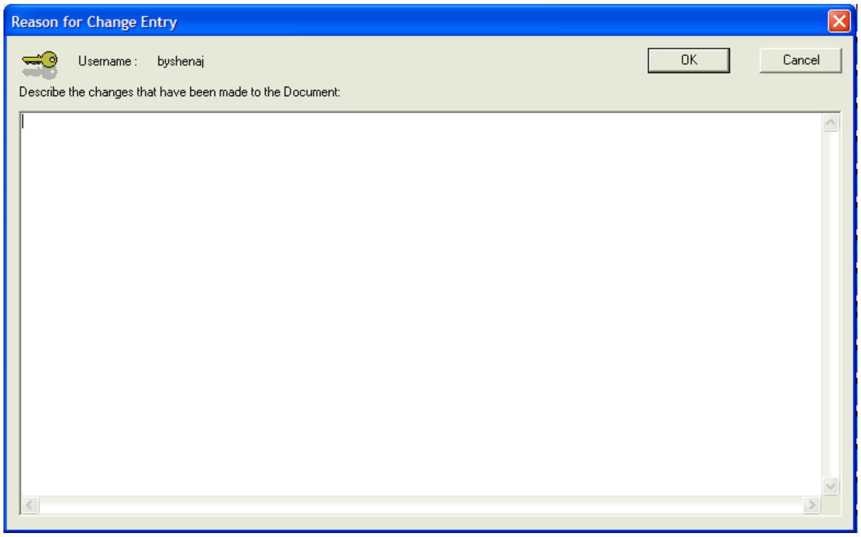
Assumptions

The procedure below assumes the following:

- Auditing is enabled for the File Type.
- Auditing is configured with *Reason For Change Optional* or *Reason For Change Required*.
- You have permission to perform the desired Controlled Activities.

Recording Changes

1. Create, update, or delete an *.sds, *.sdm, or *.sdt file.
2. When you are done, click 💾 (**Save Document**) or select **File** ▸ **Save** to save your changes. The Reason for Change Entry dialog box is displayed.

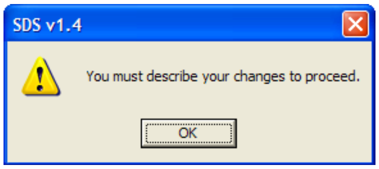


Username : byshenaj

Describe the changes that have been made to the Document:

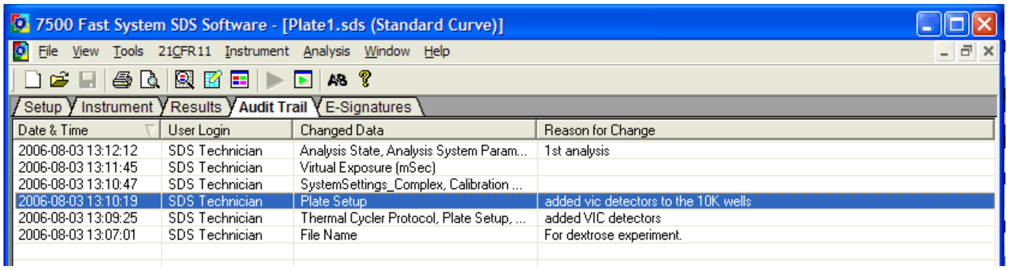
3. Complete the text field:
   - If the SDS Software System Administrator configured the data auditing as *Reason For Change Optional*, you can enter a reason for the change in the text field or leave the field empty.

- If the SDS Software System Administrator configured the data auditing as *Reason For Change Required*, you must type a reason for the change in the text field. If you click **OK** in the Reason for Change Entry dialog box without entering text in the field, the error message below is displayed. The SDS Software will not proceed until you enter text in the field.


SDS v1.4

You must describe your changes to proceed.

4. Click **OK** to close the Reason for Change Entry dialog box. The SDS Software records the text you entered in the Reason for Change Entry dialog box in the file's Individual Audit Trail, under the Reason for Change column. (See "Viewing an Individual Audit Trail" on page 53 for a description of the audit trail information.)


7500 Fast System SDS Software - [Plate1.sds (Standard Curve)]

Date & Time	User Login	Changed Data	Reason for Change
2006-08-03 13:12:12	SDS Technician	Analysis State, Analysis System Param...	1st analysis
2006-08-03 13:11:45	SDS Technician	Virtual Exposure (mSec)	
2006-08-03 13:10:47	SDS Technician	SystemSettings_Complex, Calibration ...	
2006-08-03 13:10:19	SDS Technician	Plate Setup	added vic detectors to the 10K wells
2006-08-03 13:09:25	SDS Technician	Thermal Cycler Protocol, Plate Setup, ...	added VIC detectors
2006-08-03 13:07:01	SDS Technician	File Name	For dextrose experiment.

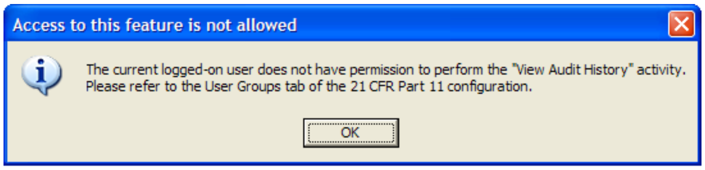
Viewing Audit Trails

User Group Permission

To perform the procedures in this section, you must log in to the SDS Software as a member of a User Group that has permission to perform the *View Audit History* Controlled Activity.

Viewing the Configuration Audit Trail

1. In the SDS Software main menu, select **21CFR11** ▸ **Configuration Audit Trail** to open the System Audit window. If you do not have permission to perform the *View Audit History* Controlled Activity, the alert message below is displayed.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "View Audit History" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

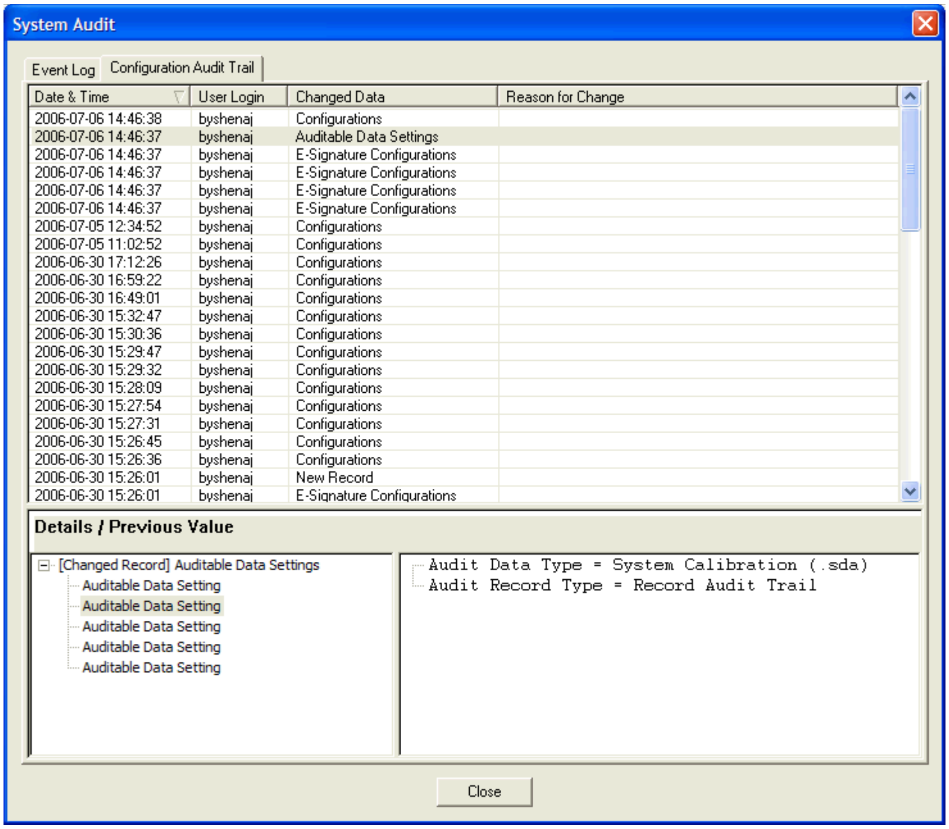
2. Select the **Configuration Audit Trail** tab (default).

Notes

Information in the Configuration Audit Trail

- **Date & Time** – The date and time the change occurred.
- **User Login** – The name on the logged-in user account when the change occurred. The user account's login name is recorded here, rather than the full name.
- **Changed Data** – The type of data that was affected by the change.
- **Reason for Change** – This field is empty (blank). The system configuration data is audited silently; users cannot enter a reason for changing system configuration data.
- **Details/Previous Value** – The previous value of the changed data. In the left pane, each item affected by the change is labeled with *Changed Record, Added Record,* or *Deleted Record*.

Note: Select a row in the upper pane to view the previous value for that data in the Previous Value pane.



Date & Time	User Login	Changed Data	Reason for Change
2006-07-06 14:46:38	byshenaj	Configurations	
2006-07-06 14:46:37	byshenaj	Auditable Data Settings	
2006-07-06 14:46:37	byshenaj	E-Signature Configurations	
2006-07-06 14:46:37	byshenaj	E-Signature Configurations	
2006-07-06 14:46:37	byshenaj	E-Signature Configurations	
2006-07-06 14:46:37	byshenaj	E-Signature Configurations	
2006-07-05 12:34:52	byshenaj	Configurations	
2006-07-05 11:02:52	byshenaj	Configurations	
2006-06-30 17:12:26	byshenaj	Configurations	
2006-06-30 16:59:22	byshenaj	Configurations	
2006-06-30 16:49:01	byshenaj	Configurations	
2006-06-30 15:32:47	byshenaj	Configurations	
2006-06-30 15:30:36	byshenaj	Configurations	
2006-06-30 15:29:47	byshenaj	Configurations	
2006-06-30 15:29:32	byshenaj	Configurations	
2006-06-30 15:28:09	byshenaj	Configurations	
2006-06-30 15:27:54	byshenaj	Configurations	
2006-06-30 15:27:31	byshenaj	Configurations	
2006-06-30 15:26:45	byshenaj	Configurations	
2006-06-30 15:26:36	byshenaj	Configurations	
2006-06-30 15:26:01	byshenaj	New Record	
2006-06-30 15:26:01	byshenaj	E-Signature Configurations	

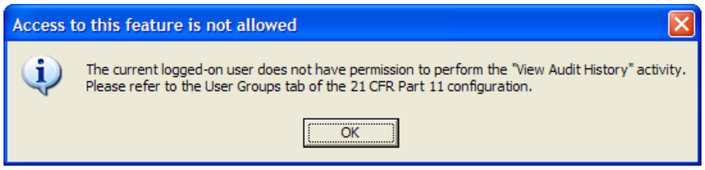
Details / Previous Value

```
⊟ [Changed Record] Auditable Data Settings
    Auditable Data Setting
    Auditable Data Setting
    Auditable Data Setting
    Auditable Data Setting
    Auditable Data Setting
```

```
Audit Data Type = System Calibration (.sda)
Audit Record Type = Record Audit Trail
```

Viewing the Event Log

1. In the SDS Software main menu, select **21CFR11 ▸ System Event Log** to open the System Audit window. If you do not have permission to perform the *View Audit History* Controlled Activity, the alert message below is displayed.



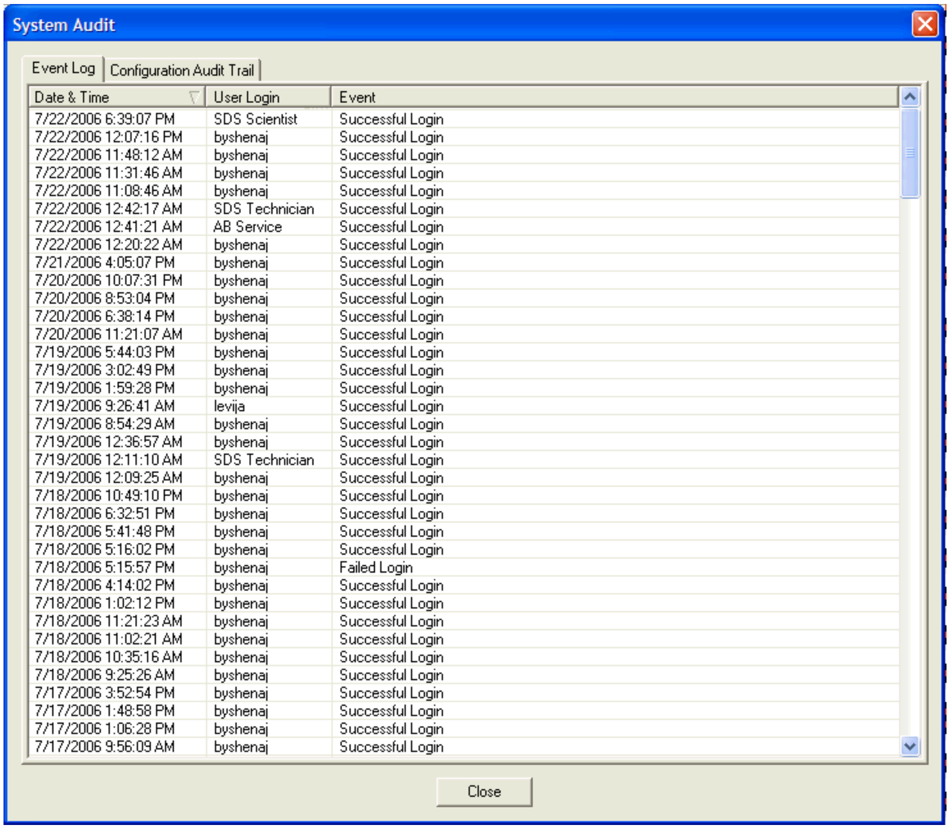
Access to this feature is not allowed

The current logged-on user does not have permission to perform the "View Audit History" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

2. Select the **Event Log** tab (default).

Information in the Event Log

- **Date & Time** – The date and time the event occurred.
- **User Login** – The name on the logged-in user account when the event occurred. The user account's login name is recorded here, rather than the full name.
- **Event** – The event that occurred: *Failed E-Signature*, *Failed Login,* or *Successful Login*.

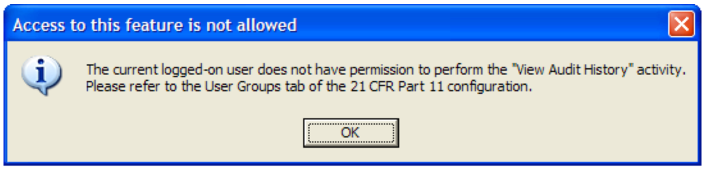


Date & Time	User Login	Event
7/22/2006 6:39:07 PM	SDS Scientist	Successful Login
7/22/2006 12:07:16 PM	byshenaj	Successful Login
7/22/2006 11:48:12 AM	byshenaj	Successful Login
7/22/2006 11:31:46 AM	byshenaj	Successful Login
7/22/2006 11:08:46 AM	byshenaj	Successful Login
7/22/2006 12:42:17 AM	SDS Technician	Successful Login
7/22/2006 12:41:21 AM	AB Service	Successful Login
7/22/2006 12:20:22 AM	byshenaj	Successful Login
7/21/2006 4:05:07 PM	byshenaj	Successful Login
7/20/2006 10:07:31 PM	byshenaj	Successful Login
7/20/2006 8:53:04 PM	byshenaj	Successful Login
7/20/2006 6:38:14 PM	byshenaj	Successful Login
7/20/2006 11:21:07 AM	byshenaj	Successful Login
7/19/2006 5:44:03 PM	byshenaj	Successful Login
7/19/2006 3:02:49 PM	byshenaj	Successful Login
7/19/2006 1:59:28 PM	byshenaj	Successful Login
7/19/2006 9:26:41 AM	levija	Successful Login
7/19/2006 8:54:29 AM	byshenaj	Successful Login
7/19/2006 12:36:57 AM	byshenaj	Successful Login
7/19/2006 12:11:10 AM	SDS Technician	Successful Login
7/19/2006 12:09:25 AM	byshenaj	Successful Login
7/18/2006 10:49:10 PM	byshenaj	Successful Login
7/18/2006 6:32:51 PM	byshenaj	Successful Login
7/18/2006 5:41:48 PM	byshenaj	Successful Login
7/18/2006 5:16:02 PM	byshenaj	Successful Login
7/18/2006 5:15:57 PM	byshenaj	Failed Login
7/18/2006 4:14:02 PM	byshenaj	Successful Login
7/18/2006 1:02:12 PM	byshenaj	Successful Login
7/18/2006 11:21:23 AM	byshenaj	Successful Login
7/18/2006 11:02:21 AM	byshenaj	Successful Login
7/18/2006 10:35:16 AM	byshenaj	Successful Login
7/18/2006 9:25:26 AM	byshenaj	Successful Login
7/17/2006 3:52:54 PM	byshenaj	Successful Login
7/17/2006 1:48:58 PM	byshenaj	Successful Login
7/17/2006 1:06:28 PM	byshenaj	Successful Login
7/17/2006 9:56:09 AM	byshenaj	Successful Login

Notes

Viewing the Calibration Audit Trail

1. In the SDS Software main menu, select **21CFR11 ▸ Calibration Audit Trail** to open the Instrument window. If you do not have permission to perform the *View Audit History* Controlled Activity, the alert message below is displayed.



Access to this feature is not allowed

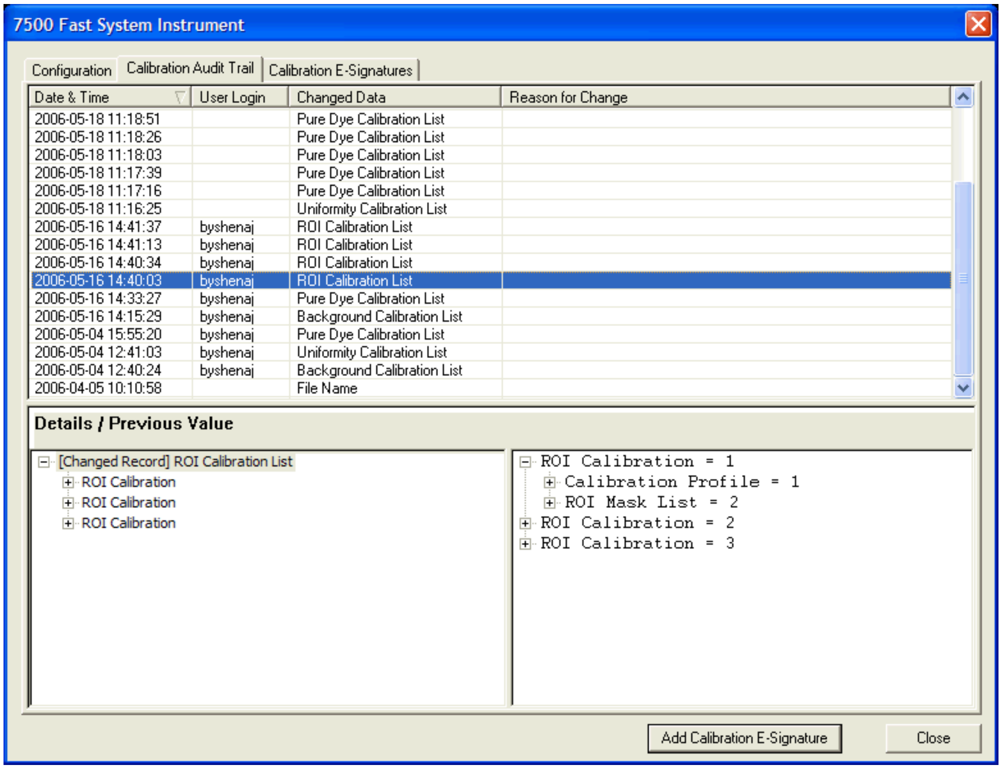
The current logged-on user does not have permission to perform the "View Audit History" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

2. Select the **Calibration Audit Trail** tab (default).

Information in the Calibration Audit Trail

- **Date & Time** – The date and time the change occurred.
- **User Login** – The name on the logged-in user account when the change occurred. The user account's login name is recorded here, rather than the full name.
- **Changed Data** – The type of data that was affected by the change.
- **Reason for Change** – This field is empty (blank). The system calibration data is audited silently; users cannot enter a reason for changing system calibration data.
- **Details/Previous Value** – The previous value of the changed data. In the left pane, each item affected by the change is labeled with *Changed Record, Added Record,* or *Deleted Record*.

Note: Select a row in the upper pane to view the previous value for that data in the Previous Value pane.



Date & Time	User Login	Changed Data	Reason for Change
2006-05-18 11:18:51		Pure Dye Calibration List	
2006-05-18 11:18:26		Pure Dye Calibration List	
2006-05-18 11:18:03		Pure Dye Calibration List	
2006-05-18 11:17:39		Pure Dye Calibration List	
2006-05-18 11:17:16		Pure Dye Calibration List	
2006-05-18 11:16:25		Uniformity Calibration List	
2006-05-16 14:41:37	byshenaj	ROI Calibration List	
2006-05-16 14:41:13	byshenaj	ROI Calibration List	
2006-05-16 14:40:34	byshenaj	ROI Calibration List	
2006-05-16 14:40:03	byshenaj	ROI Calibration List	
2006-05-16 14:33:27	byshenaj	Pure Dye Calibration List	
2006-05-16 14:15:29	byshenaj	Background Calibration List	
2006-05-04 15:55:20	byshenaj	Pure Dye Calibration List	
2006-05-04 12:41:03	byshenaj	Uniformity Calibration List	
2006-05-04 12:40:24	byshenaj	Background Calibration List	
2006-04-05 10:10:58		File Name	

Details / Previous Value

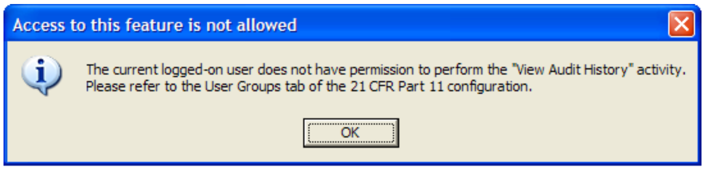
```
⊟ [Changed Record] ROI Calibration List
   ⊞ ROI Calibration
   ⊞ ROI Calibration
   ⊞ ROI Calibration
```

```
⊟ ROI Calibration = 1
   ⊞ Calibration Profile = 1
   ⊞ ROI Mask List = 2
⊞ ROI Calibration = 2
⊞ ROI Calibration = 3
```

Viewing an Individual Audit Trail

1. Open the *.sds, *.sdm, or *.sdt for which you want to view the Individual Audit Trail.

2. Select the **Audit Trail** tab. If you do not have permission to perform the *View Audit History* Controlled Activity, the alert message below is displayed.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "View Audit History" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Note: The Audit Trail tab is not available for legacy files.

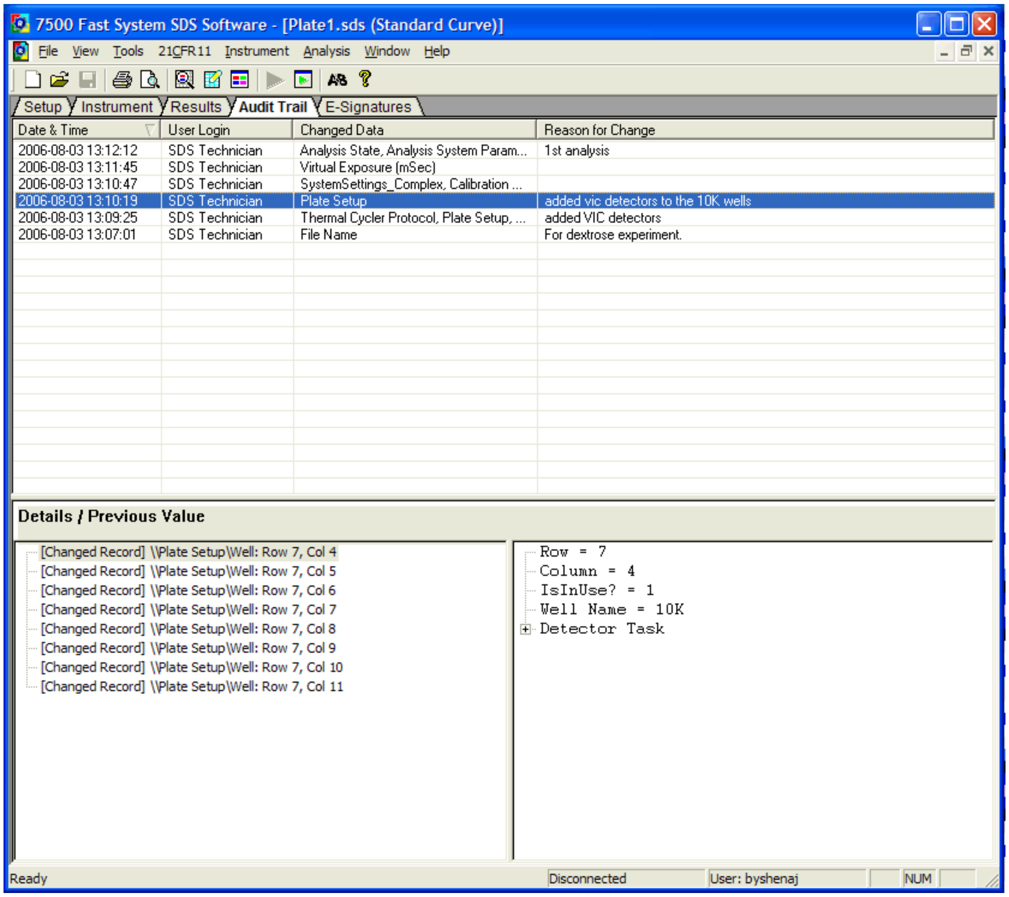
Information in the Individual Audit Trails

- **Date & Time** – The date and time the change occurred.
- **User Login** – The name on the logged-in user account when the change occurred. The user account's login name is recorded here, rather than the full name.
- **Changed Data** – The type of data that was affected by the change.
- **Reason for Change** – Any text the user may have entered in the text field of the Reason for Change Entry dialog box when making the change. (See "Recording Changes" on page 48 for more information.)

Notes

- **Details/Previous Value** – The previous value of the changed data. In the left pane, each item affected by the change is labeled with *Changed Record, Added Record,* or *Deleted Record*.

Note: Select a row in the upper pane to view the previous value for that data in the Previous Value pane.


7500 Fast System SDS Software - [Plate1.sds (Standard Curve)]
File View Tools 21CFR11 Instrument Analysis Window Help
Setup
Instrument
Results
Audit Trail
E-Signatures

Date & Time	User Login	Changed Data	Reason for Change
2006-08-03 13:12:12	SDS Technician	Analysis State, Analysis System Param...	1st analysis
2006-08-03 13:11:45	SDS Technician	Virtual Exposure (mSec)	
2006-08-03 13:10:47	SDS Technician	SystemSettings_Complex, Calibration ...	
2006-08-03 13:10:19	SDS Technician	Plate Setup	added vic detectors to the 10K wells
2006-08-03 13:09:25	SDS Technician	Thermal Cycler Protocol, Plate Setup, ...	added VIC detectors
2006-08-03 13:07:01	SDS Technician	File Name	For dextrose experiment.

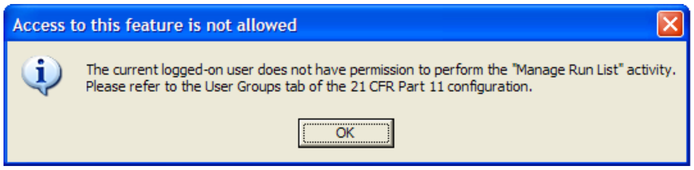
Details / Previous Value

[Changed Record] \\Plate Setup\Well: Row 7, Col 4
[Changed Record] \\Plate Setup\Well: Row 7, Col 5
[Changed Record] \\Plate Setup\Well: Row 7, Col 6
[Changed Record] \\Plate Setup\Well: Row 7, Col 7
[Changed Record] \\Plate Setup\Well: Row 7, Col 8
[Changed Record] \\Plate Setup\Well: Row 7, Col 9
[Changed Record] \\Plate Setup\Well: Row 7, Col 10
[Changed Record] \\Plate Setup\Well: Row 7, Col 11

```
Row = 7
Column = 4
IsInUse? = 1
Well Name = 10K
+ Detector Task
```

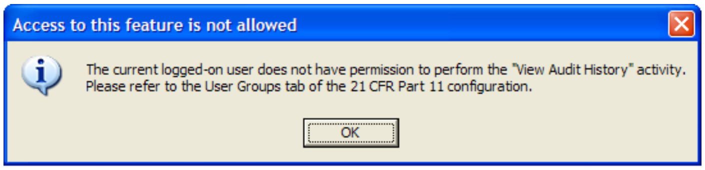
Viewing the Run List Audit Trail

1. In the SDS Software main menu, select **Tools ▸ Run List Manager** to open the Run List Manager window. If you do not have permission to perform the *Manage Run List* Controlled Activity, the alert message below is displayed.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Manage Run List" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

2. Select the **Audit Trail** tab. If you do not have permission to perform the *View Audit History* Controlled Activity, the alert message below is displayed.

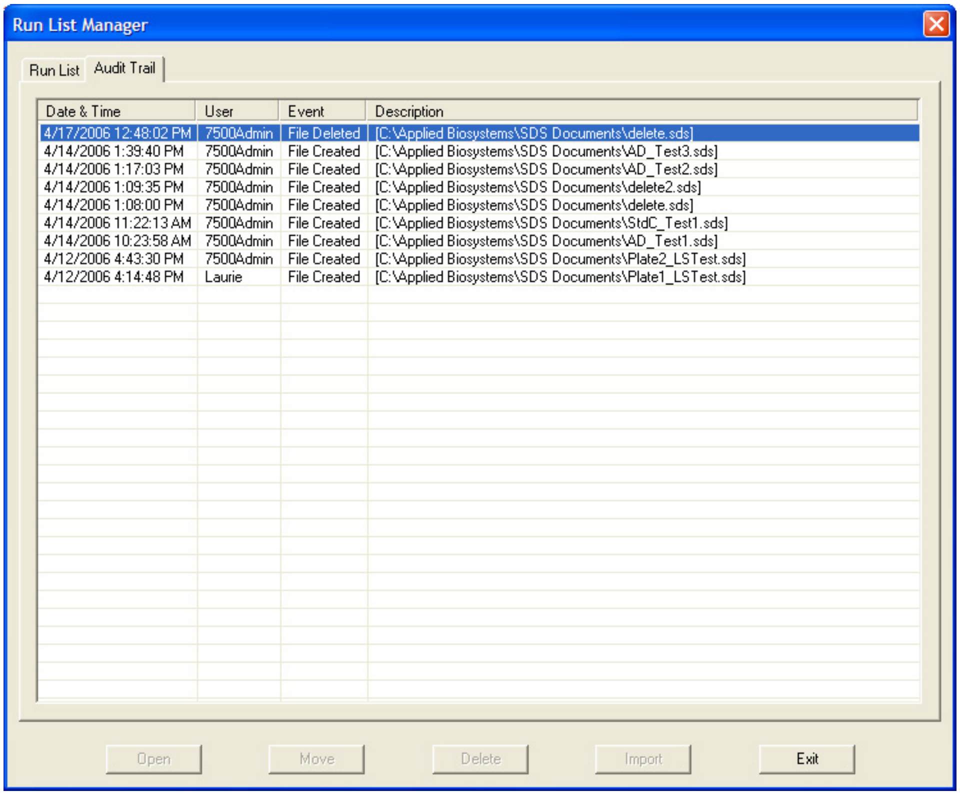

Access to this feature is not allowed

The current logged-on user does not have permission to perform the "View Audit History" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Information in the Run List Audit Trail

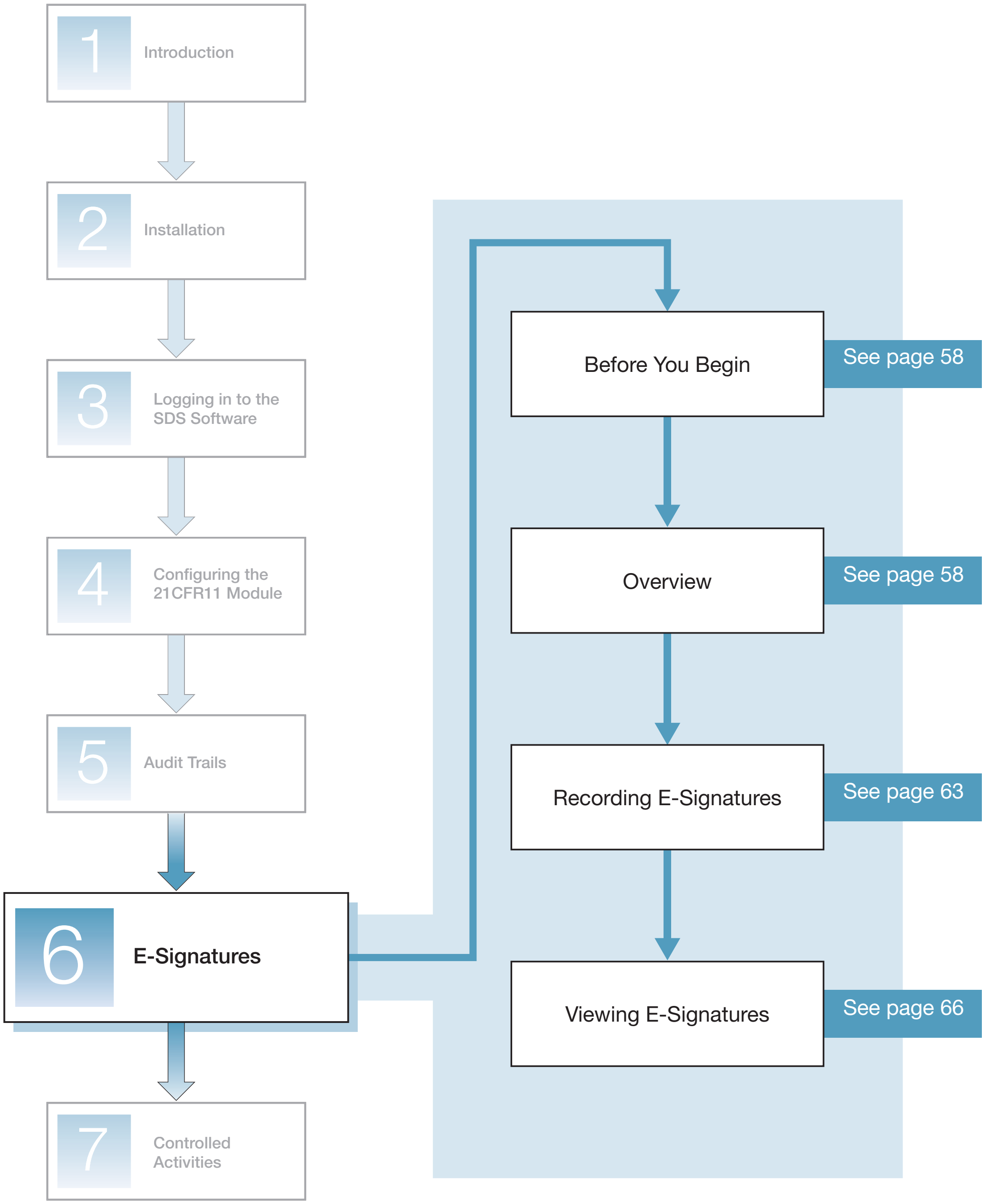
- **Date & Time** – The date and time the change occurred.
- **User Login** – The name on the logged-in user account when the change occurred. The user account's login name is recorded here, rather than the full name.
- **Event** – The change that occurred: *File Created, File Imported, File Moved, File Deleted,* or *Record Deleted*.
- **Description** – The location and name of the file that was affected.

Notes



Date & Time	User	Event	Description
4/17/2006 12:48:02 PM	7500Admin	File Deleted	[C:\Applied Biosystems\SDS Documents\delete.sds]
4/14/2006 1:39:40 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\AD_Test3.sds]
4/14/2006 1:17:03 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\AD_Test2.sds]
4/14/2006 1:09:35 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\delete2.sds]
4/14/2006 1:08:00 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\delete.sds]
4/14/2006 11:22:13 AM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\StdC_Test1.sds]
4/14/2006 10:23:58 AM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\AD_Test1.sds]
4/12/2006 4:43:30 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\Plate2_LSTest.sds]
4/12/2006 4:14:48 PM	Laurie	File Created	[C:\Applied Biosystems\SDS Documents\Plate1_LSTest.sds]

6 E-Signatures



Notes

Before You Begin

User Group Permissions

To perform the procedures in this chapter, you must log in to the SDS Software as a member of the User Group specified in each procedure. For information on configuring User Group Permissions, see page 35.

Logging In

For login procedures, see Chapter 3 on page 23.

Overview

E-Signatures are electronic signatures that can be recorded in the SDS Software to approve data associated with predefined Signing Types.

Signing Types

The table below describes the Signing Types predefined in the SDS Software.

Signing Type	File Type[‡]	Associated Data (Data Covered by the Approval)	When the Approval Can Be Performed
Approval of Acquisition Data	User Runs	Raw data collected during the run.	After the run is completed.
Approval of Analysis Results	User Runs User Studies	Analysis results.	When analysis results are available.
Approval of Analysis Settings	User Runs User Studies	• For each detector identified/defined in the plate: – Detector name – Reporter dye name – Quencher dye name – Description – Comment – Display color – Creation time stamp – Modification time stamp – Owner – Auto baseline flag setting – Auto threshold flag setting – Baseline begin cycle[§] – Baseline end cycle[§] – Threshold[#] – Quality factor • For each marker identified/define in the plate: – Marker name – Allele X name – Allele Y name – Description – Comment – Display color – Creation time stamp – Modification time stamp – Owner – Confidence – Autocall flag setting – Cluster setting	Any time.

Notes

Signing Type	File Type‡	Associated Data (Data Covered by the Approval)	When the Approval Can Be Performed
Approval of Calibration Data	User Runs System Calibration	• ROIs • Background calibration • Uniformity calibration • Pure dye calibration	Any time.
Approval of Document Submission	User Runs User Studies Templates System Calibration	All data in the file.	Any time.
Approval of Plate Setup	User Runs Templates	• For each well in the plate: – Sample name – Description • For each detector in the well: – Detector name – Task – Quantity (AQ) – Markers (AD)	Any time.
Approval of Thermal Cycler Program	User Runs Templates	• The method run by the instrument • The global reaction volume • The data collection step indicator • The Expert Mode settings (collected filters)	Any time.

‡ There are no predefined Signing Types for the *System Configuration* or *System Run List* File Types.
§ The *Baseline begin cycle* and *Baseline end cycle* values are included only if the Auto baseline flag is false.
# The *Threshold* value is included only if the Auto threshold flag is false.

When recording an E-Signature, the user is approving the current data associated with the Signing Type. For example, if a user signs for *Approval of Plate Setup*, the current well and detector information listed above is approved for the *.sds or *.sdt file.

IMPORTANT! When a user records an E-Signature for *Approval of Document Submission*, all current data in the file is approved.

E-Signatures Configuration

The SDS Software System Administrator can configure E-Signatures as follows:

- For each File Type (User Runs, User Studies, Templates, and System Calibration), E-Signatures can be enabled or disabled.

  Note: Data auditing must also be enabled for a File Type in order to record E-Signatures for that File Type.

- For each Signing Type within the File Type, an E-Signature can be optional or required:
  - If an E-Signature is optional, a user may or may not record an E-Signature for the Signing Type. The SDS Software proceeds without interruption.
  - If an E-Signature is required, a user must record an E-Signature for the Signing Type. Otherwise, the SDS Software restricts further action(s) related to the Signing Type. For a list of restrictions, see "Restrictions for Required E-Signatures" on page 61.
- When E-Signatures are enabled, the E-Signature information is recorded as follows:
  - For the User Runs, User Studies, and Templates File Types, the information is recorded in the E-Signatures tab within the *.sds, *.sdm, or *.sdt file.
  - For the System Calibration File Type, the information is recorded in the Calibration E-Signatures tab within the Instrument window.

Note: For information on configuring E-Signatures, see page 40.

Restrictions for Required E-Signatures

If the SDS Software System Administrator configures a Signing Type to *require* an E-Signature, a user must record an E-Signature for the Signing Type. Otherwise, the SDS Software restricts further action(s) related to the Signing Type (as described in the table below) and displays an error message describing the condition.

Note: If an E-Signature is optional for the Signing Activity, the SDS Software proceeds, whether or not a current E-Signature is recorded. If an E-Signature is required for the Signing Activity and there is already a current E-Signature recorded, the SDS Software proceeds.

File Type	Signing Type	Restriction(s) for Required E-Signatures
User Runs	Approval of Document Submission‡	There are no restrictions.
	Approval of Analysis Results	The data cannot be printed or exported.
	Approval of Analysis Settings	Analysis cannot be performed. The data cannot be printed or exported.
	Approval of Calibration Data	Results cannot be generated. The data cannot be printed or exported.
	Approval of Acquisition Data	Results cannot be generated. The data cannot be printed or exported.
	Approval of Thermal Cycler Program	The run cannot be started. The data cannot be printed or exported.
	Approval of Plate Setup	Results cannot be generated. The data cannot be printed or exported.
User Studies	Approval of Document Submission‡	There are no restrictions.
	Approval of Analysis Results	The data cannot be printed or exported.
	Approval of Analysis Settings	Analysis cannot be performed. The data cannot be printed or exported.
Templates	Approval of Document Submission	There are no restrictions.
	Approval of Thermal Cycler Program	The template cannot be used to create a run. The data cannot be printed or exported.
	Approval of Plate Setup	The template cannot be used to create a run. The data cannot be printed or exported.
System Calibration	Approval of Calibration Data	No runs can be started.
	Approval of Document Submission‡	There are no restrictions.

‡ When a user records an E-Signature for *Approval of Document Submission*, all current data in the file is approved.

Notes

Example: Starting a Run

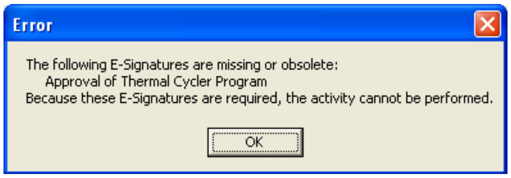
The 7500/7500 Fast Real-Time PCR System uses the following data to perform a run:

- Thermal cycler program data
- System calibration data

There are two Signing Types that include this data:

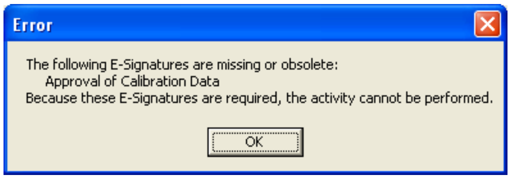
File Type	Signing Type
User Runs	Approval of Thermal Cycler Program
System Calibration	Approval of Calibration Data

If either Signing Type (*Approval of Thermal Cycler Program* or *Approval of Calibration Data*) is configured to require an E-Signature and a current E-Signature is not recorded for the Signing Type, the SDS Software cannot use the data. The SDS Software does not allow the user to start the run and displays one of the error messages shown below.



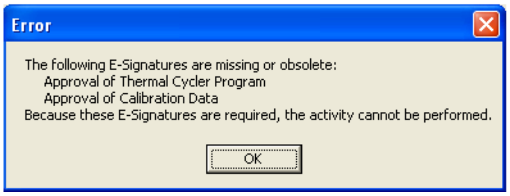
The following E-Signatures are missing or obsolete:
Approval of Thermal Cycler Program
Because these E-Signatures are required, the activity cannot be performed.

This error message is displayed if an E-Signature is required but not recorded for the *Approval of Thermal Cycler Program* Signing Type.



The following E-Signatures are missing or obsolete:
Approval of Calibration Data
Because these E-Signatures are required, the activity cannot be performed.

This error message is displayed if an E-Signature is required but not recorded for the *Approval of Calibration Data* Signing Type.



The following E-Signatures are missing or obsolete:
Approval of Thermal Cycler Program
Approval of Calibration Data
Because these E-Signatures are required, the activity cannot be performed.

This error message is displayed if an E-Signature is required but not recorded for both the *Approval of Thermal Cycler Program* and *Approval of Calibration Data* Signing Types.

Notes

Recording E-Signatures

The SDS Software does not prompt users to record E-Signatures, even when a Signing Type is configured to require an E-Signature. As described in the following procedures, you must manually access the Electronic Signatures dialog box:

- For the User Runs, User Studies, and Templates File Types, see page 63.
- For the System Calibration File Type, see page 65.

IMPORTANT! Though you do not receive a prompt when an E-Signature is required, the SDS Software restricts further action(s) related to the Signing Type until an E-Signature is obtained. If you attempt to use data that requires an E-Signature and no current E-Signature exists, the SDS Software displays an error message describing the condition. For more information, see "Restrictions for Required E-Signatures" on page 61.

User Group Permissions

Only users who are members of the SDS ESignature User Group are allowed to record E-Signatures.

Assumptions

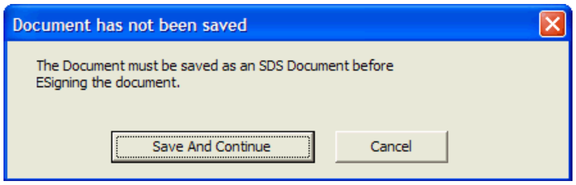
The procedures below assume the following:

- Data auditing is enabled for the File Type.
- E-Signatures have been configured as either *Optional* or *Required*.

For User Runs, User Studies, and Templates

1. Open the *.sds, *.sdm, or *.sdt for which you want to approve a Signing Type.
2. In the SDS Software main menu, select **21CFR11 ▸ Enter E-Signature**.

   Note: If changes have been made to the file but not yet saved, the error message at right is displayed. You will not be allowed to record an E-Signature until you click **Save And Continue**.

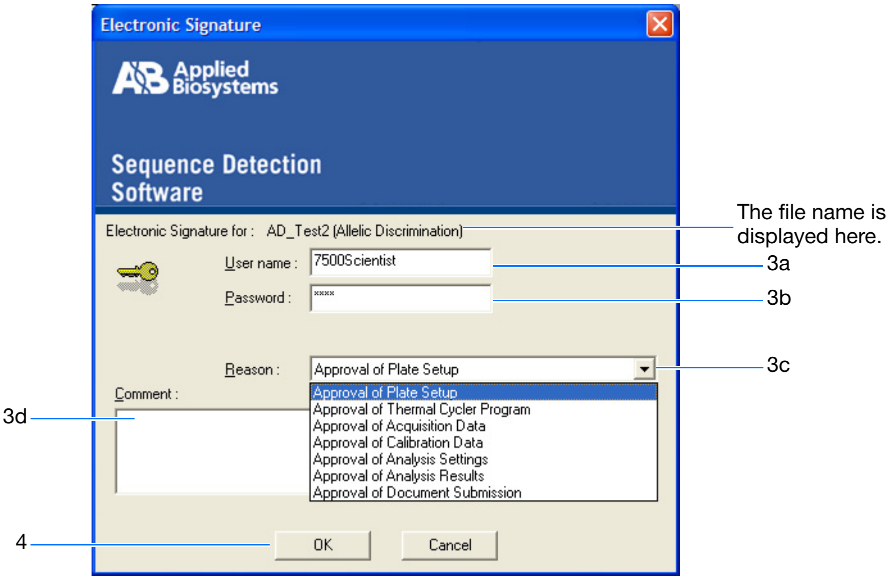
   
   Document has not been saved

   The Document must be saved as an SDS Document before ESigning the document.

3. Complete the Electronic Signature dialog box:
   a. In the User name field, enter your login name (for example, **7500Scientist**).
   b. Enter your Password.
   c. Select a Signing Type from the Reason drop-down list.

   Note: If the SDS Software System Administrator configured the Reason For Change for a Signing Type as not optional *and* not required, the Signing Type will not appear in the Reason drop-down list.

   d. (Optional) Enter a comment.



Electronic Signature for : AD_Test2 (Allelic Discrimination)

User name : 7500Scientist

Password : ****

Reason : Approval of Plate Setup

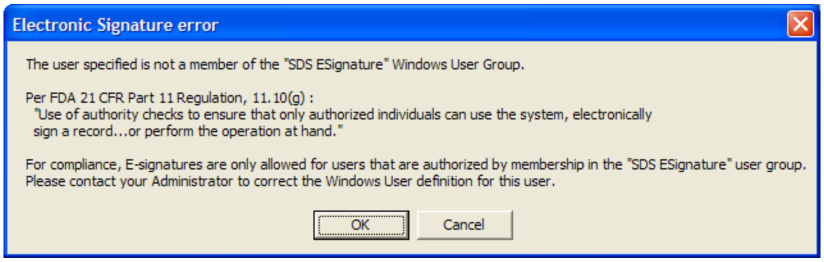
- Approval of Plate Setup
- Approval of Thermal Cycler Program
- Approval of Acquisition Data
- Approval of Calibration Data
- Approval of Analysis Settings
- Approval of Analysis Results
- Approval of Document Submission

Comment :

Note: The Electronic Signature dialog box shown above is for *.sds files. The Electronic Signature dialog boxes for *.sdm and *.sdt files display different Signing Types in the Reason drop-down menu.

4. Click **OK**:

   - If you are not a member of the SDS ESignature User Group, the alert message below is displayed.

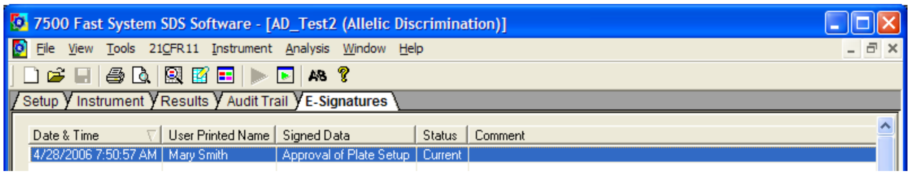


The user specified is not a member of the "SDS ESignature" Windows User Group.

Per FDA 21 CFR Part 11 Regulation, 11.10(g) :
"Use of authority checks to ensure that only authorized individuals can use the system, electronically
sign a record...or perform the operation at hand."

For compliance, E-signatures are only allowed for users that are authorized by membership in the "SDS ESignature" user group.
Please contact your Administrator to correct the Windows User definition for this user.

   - If you are a member of the SDS ESignature User Group, the SDS Software records the E-Signature information in the E-Signatures tab of the *.sds, *.sdm, or *.sdt file. (See "For User Runs, User Studies, and Templates" on page 66 for a description of the E-Signature information.)



Date & Time	User Printed Name	Signed Data	Status	Comment
4/28/2006 7:50:57 AM	Mary Smith	Approval of Plate Setup	Current	

For System Calibration

1. In the SDS Software main menu, select **21CFR11 ▸ Calibration E-Signatures** to open the Instrument window.

2. Select the tab **Calibration E-Signatures** tab (default).

3. Click **Add Calibration E-Signature**.

4. In the Electronic Signature dialog box:

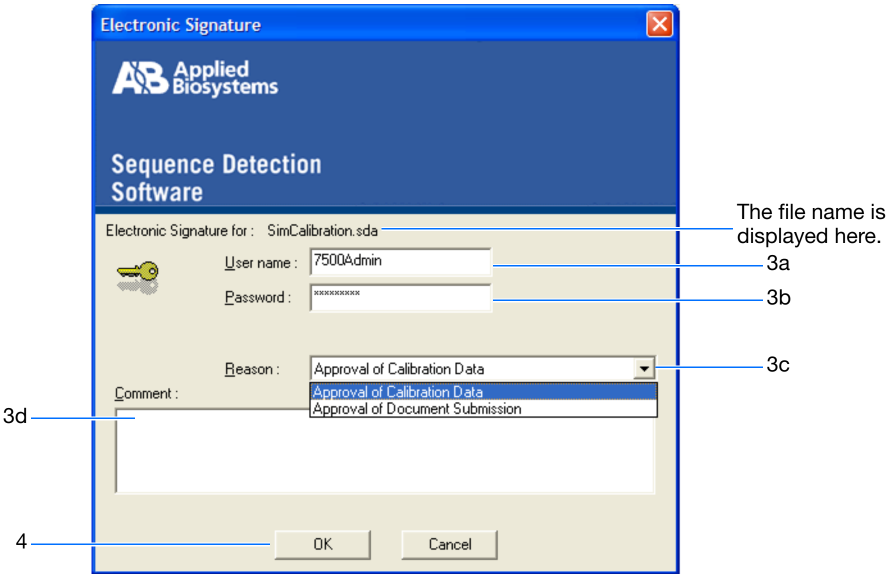
   a. In the User name field, enter your login name (for example, **7500Admin**).

   b. Enter your Password.

   c. Select a Signing Type from the Reason drop-down list.

   Note: If the SDS Software System Administrator configured the Reason For Change for a Signing Type as not optional *and* not required, the Signing Type will not appear in the Reason drop-down list.

   d. (Optional) Enter a comment.



Electronic Signature

Sequence Detection Software

Electronic Signature for : SimCalibration.sda

User name : 7500Admin

Password : *********

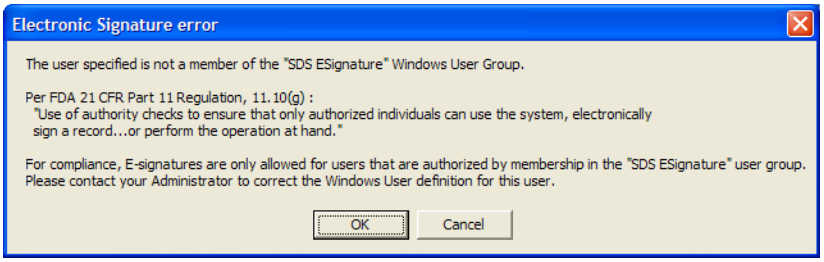
Reason : Approval of Calibration Data

Comment :

The file name is displayed here.

5. Click **OK**:

   - If you are not a member of the SDS ESignature User Group, the alert message below is displayed.



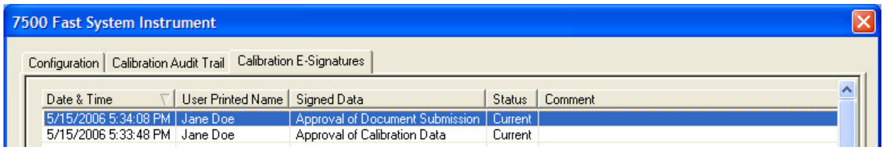
Electronic Signature error

The user specified is not a member of the "SDS ESignature" Windows User Group.

Per FDA 21 CFR Part 11 Regulation, 11.10(g) :
"Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record...or perform the operation at hand."

For compliance, E-signatures are only allowed for users that are authorized by membership in the "SDS ESignature" user group.
Please contact your Administrator to correct the Windows User definition for this user.

- If you are a member of the SDS ESignature User Group, the SDS Software records the E-Signature information in the Calibration E-Signatures tab of the Instrument window. (See "For System Calibration" on page 69 for a description of the E-Signature information.)



7500 Fast System Instrument

Date & Time	User Printed Name	Signed Data	Status	Comment
5/15/2006 5:34:08 PM	Jane Doe	Approval of Document Submission	Current	
5/15/2006 5:33:48 PM	Jane Doe	Approval of Calibration Data	Current	

Viewing E-Signatures

User Group Permission

All users are allowed to view the E-Signatures for the User Runs, User Studies, Templates, and System Calibration File Types.

For User Runs, User Studies, and Templates

1. Open the *.sds, *.sdm, or *.sdt for which you want to view the E-Signatures.
2. Select the **E-Signatures** tab.

Note: The E-Signatures tab is not available for legacy files.

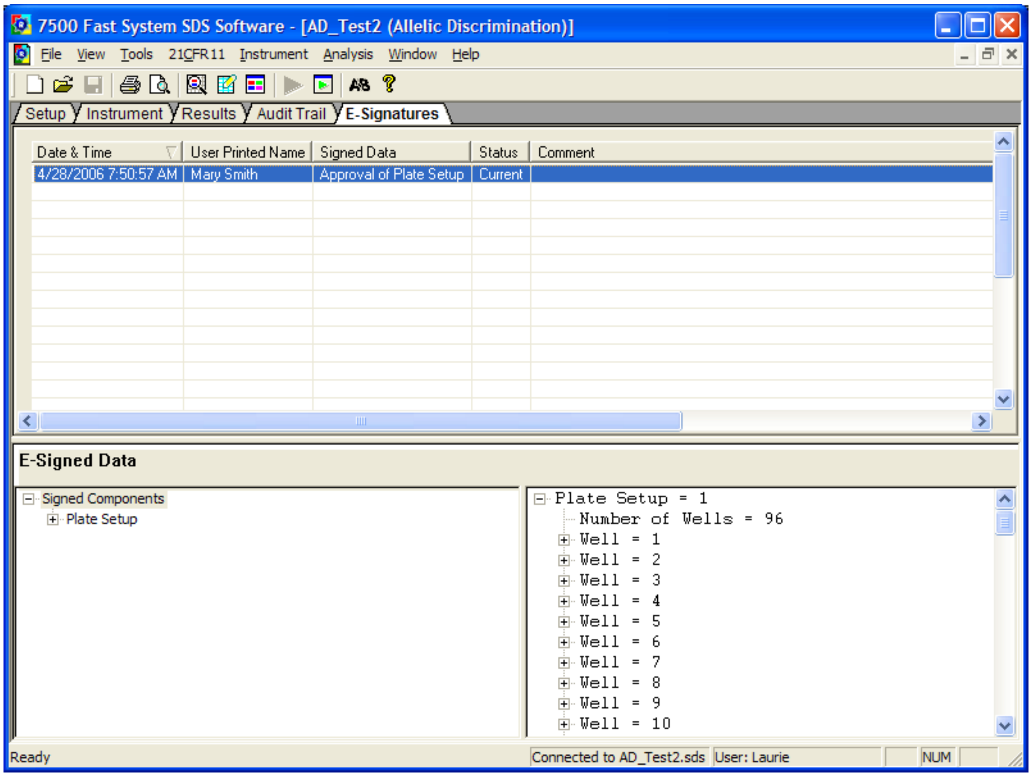
Information in the E-Signatures Tab

- **Date & Time** – The date and time the E-Signature was recorded.
- **User Printed Name** – The user who recorded the E-Signature. The user's full name is recorded here, rather than the user's login name.

- **Signed Data** – The Signing Type for which the E-Signature was recorded:

File Type	Signing Type
User Runs	Approval of Document Submission
	Approval of Analysis Results
	Approval of Analysis Settings
	Approval of Calibration Data
	Approval of Acquisition Data
	Approval of Thermal Cycler Program
	Approval of Plate Setup
User Studies	Approval of Document Submission
	Approval of Analysis Results
	Approval of Analysis Settings
Templates	Approval of Document Submission
	Approval of Thermal Cycler Program
	Approval of Plate Setup

- **Status** – The status of the data for which the E-Signature was recorded: *Current* or *Obsolete*. *Obsolete* indicates that the data has been superseded by newer data.
- **Comment** – Any text the user may have entered in the Comment field of the Electronic Signatures dialog box.
- **E-Signed Data pane** – Displays the details of the signed data. (Select a row in the upper pane to view the details for that data in the E-Signed Data pane.)


7500 Fast System SDS Software - [AD_Test2 (Allelic Discrimination)]
File View Tools 21CFR11 Instrument Analysis Window Help
Setup
Instrument
Results
Audit Trail
E-Signatures

Date & Time	User Printed Name	Signed Data	Status	Comment
4/28/2006 7:50:57 AM	Mary Smith	Approval of Plate Setup	Current	

E-Signed Data

- Signed Components
  - Plate Setup

```
Plate Setup = 1
  Number of Wells = 96
  Well = 1
  Well = 2
  Well = 3
  Well = 4
  Well = 5
  Well = 6
  Well = 7
  Well = 8
  Well = 9
  Well = 10
```

Ready
Connected to AD_Test2.sds
User: Laurie
NUM

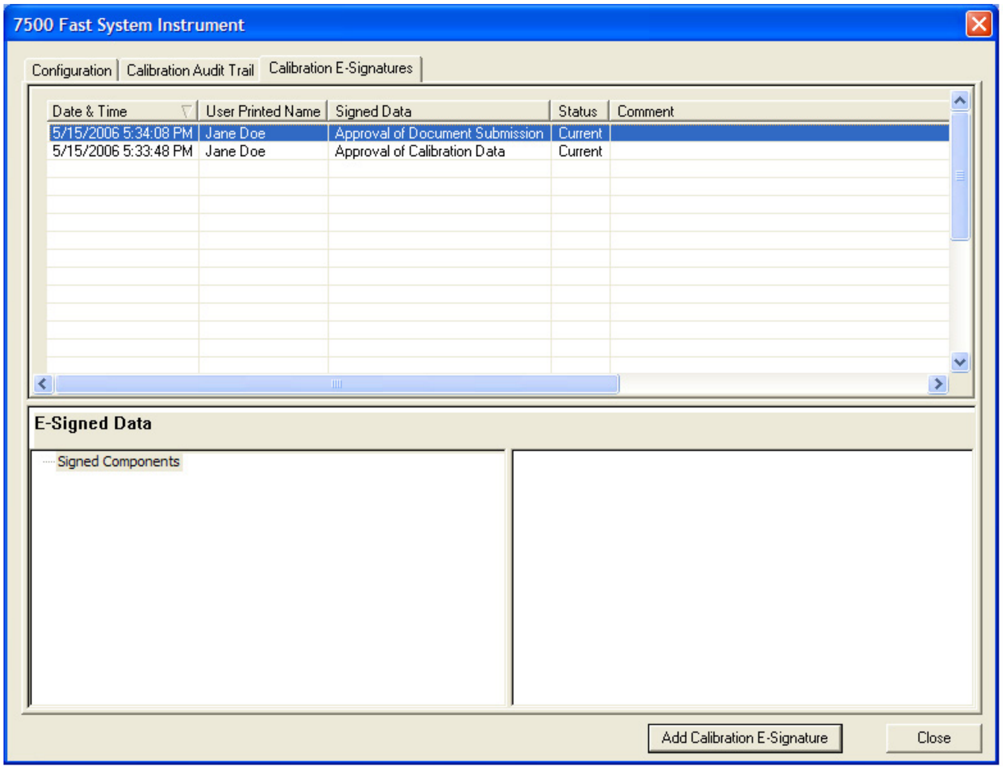
For System Calibration

1. In the SDS Software main menu, select **21CFR11 ▸ Calibration E-Signatures** to open the Instrument window.

2. Select the tab **Calibration E-Signatures** tab (default).

Information in the Calibration E-Signatures Tab

- **Date & Time** – The date and time the E-Signature was recorded.
- **User Printed Name** – The user who recorded the E-Signature. The user’s full name is recorded here, rather than the user’s login name.
- **Signed Data** – The Signing Type for which the E-Signature was recorded: *Approval of Calibration Data* and *Approval of Document Submission*.
- **Status** – The status of the data for which the E-Signature was recorded: *Current* or *Obsolete*. *Obsolete* indicates that the data has been superseded by newer data.
- **Comment** – Any text the user may have entered in the Comment field of the Electronic Signatures dialog box.
- **E-Signed Data pane** – Displays the details of the signed data. (Select a row in the upper pane to view the details for that data in the E-Signed Data pane.)



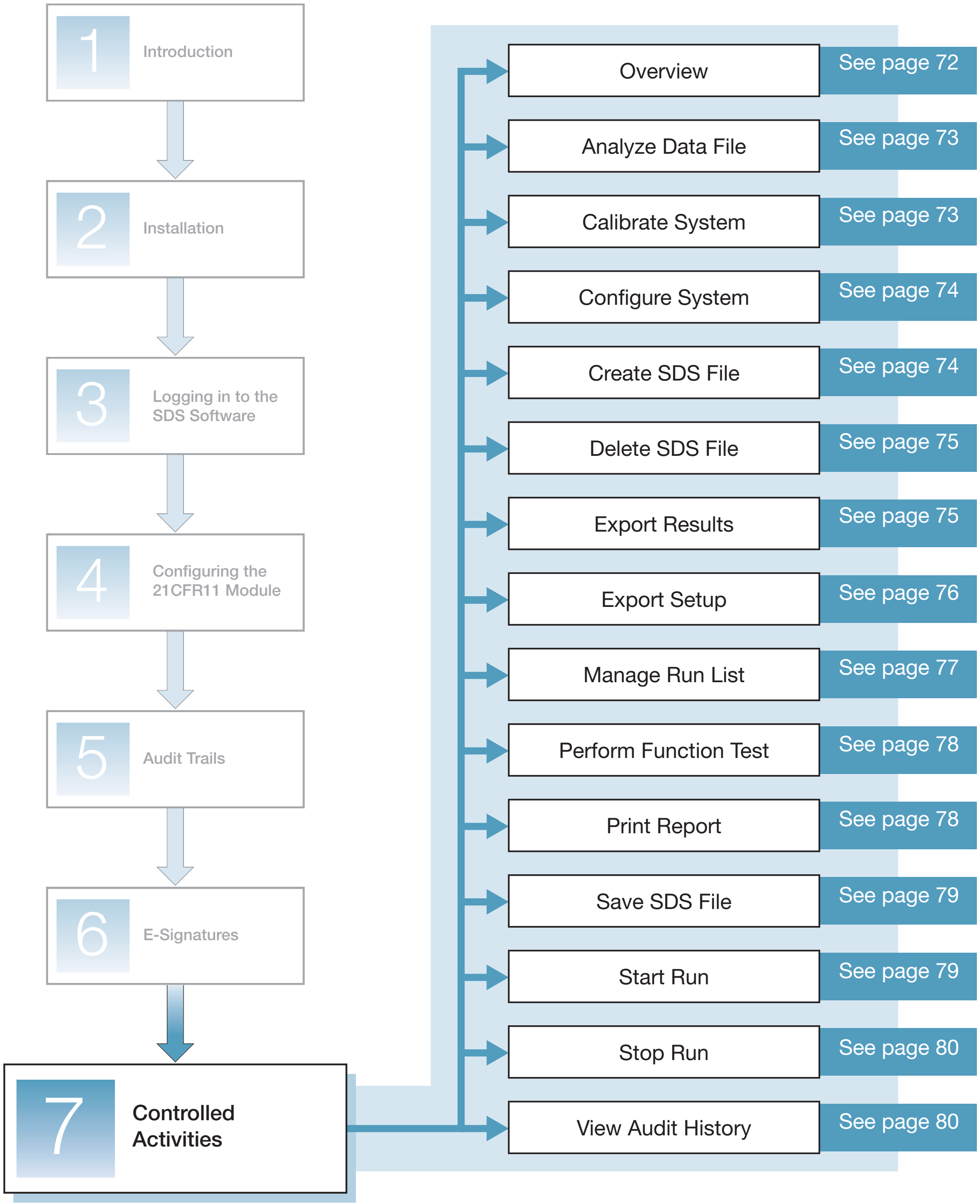
Date & Time	User Printed Name	Signed Data	Status	Comment
5/15/2006 5:34:08 PM	Jane Doe	Approval of Document Submission	Current	
5/15/2006 5:33:48 PM	Jane Doe	Approval of Calibration Data	Current	

Notes

Notes

7

Controlled Activities



Overview See page 72
Analyze Data File See page 73
Calibrate System See page 73
Configure System See page 74
Create SDS File See page 74
Delete SDS File See page 75
Export Results See page 75
Export Setup See page 76
Manage Run List See page 77
Perform Function Test See page 78
Print Report See page 78
Save SDS File See page 79
Start Run See page 79
Stop Run See page 80
View Audit History See page 80

Notes

Overview

Within the SDS Software, Controlled Activities are operations that users can either be allowed to perform or prevented from performing. A user's access to a Controlled Activity is based on the User Group(s) to which he or she belongs. Each of the Controlled Activities within the SDS Software can be permitted to any combination of the following User Groups:

- SDS Administrators
- SDS Scientists
- SDS Technicians
- SDS Service

Note: For information on assigning users to User Groups, see "Creating Users and User Groups in the Operating System" on page 12. For information on assigning Controlled Activities to User Groups, see "Configuring User Group Permissions" on page 35.

Controlled Activities

The following Controlled Activities are predefined in the SDS Software:

- Analyze Data File (page 73)
- Calibrate System (page 73)
- Configure System (page 74)
- Create SDS File (page 74)
- Delete SDS File (page 75)
- Export Results (page 75)
- Export Setup (page 76)
- Manage Run List (page 77)
- Perform Function Test (page 78)
- Print Report (page 78)
- Save SDS File (page 79)
- Start Run (page 79)
- Stop Run (page 80)
- View Audit History (page 80)

Information in This Chapter

This chapter describes:

- The function of each Controlled Activity.
- The User Group permission required to perform each Controlled Activity.

With the exception of *Configure System* and *View Audit History*, procedures for performing the Controlled Activities are not provided in this document.

- For procedures on performing the *Configure System* Controlled Activity, see "Configuring the 21CFR11 Module" on page 31.

Notes

- For procedures on performing the *View Audit History* Controlled Activity, see "Viewing Audit Trails" on page 49.
- For procedures on performing the remaining Controlled Activities, see the *SDS Online Help* and the assay *Getting Started Guides*.

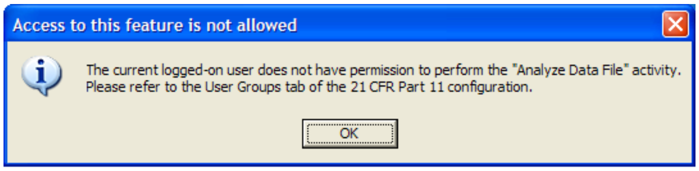
Analyze Data File

The *Analyze Data File* Controlled Activity controls the ability of users to analyze the User Runs File Type.

User Group Permission

The user must belong to a User Group that has permission to perform the *Analyze Data File* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot analyze the file.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Analyze Data File" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

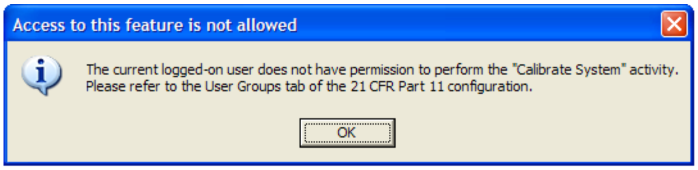
Calibrate System

The *Calibrate System* Controlled Activity controls the ability of users to calibrate the Real-Time PCR System.

User Group Permission

The user must belong to a User Group that has permission to perform the *Calibrate System* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot calibrate the Real-Time PCR System.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Calibrate System" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Notes

Configure System

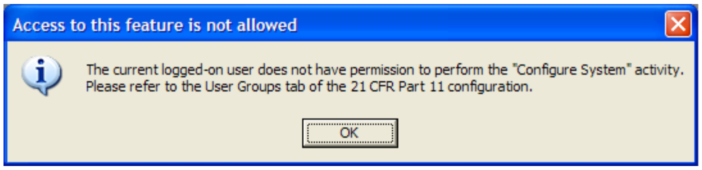
The *Configure System* Controlled Activity controls the ability of users to configure the 21CFR11 module in the SDS Software.

Note: For procedures on performing the *Configure System* Controlled Activity, see "Configuring the 21CFR11 Module" on page 31.

User Group Permission

The user must belong to a User Group that has permission to perform the *Configure System* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot configure the 21CFR11 module.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Configure System" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

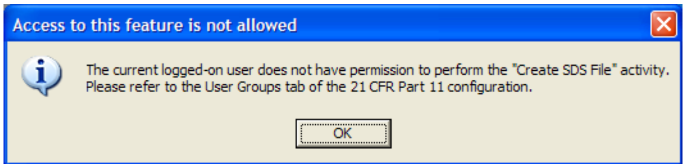
Create SDS File

The *Create SDS File* Controlled Activity controls the ability of users to create the User Runs, User Studies, and Templates File Types.

User Group Permissions

The user must belong to a User Group that has permission to perform the *Create SDS File* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot create a file.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Create SDS File" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Notes

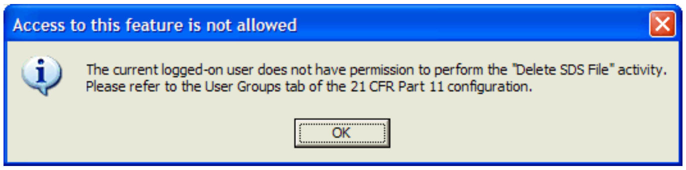
Delete SDS File

The *Delete SDS File* Controlled Activity controls the ability of users to delete the User Runs, User Studies, and Templates File Types.

User Group Permissions

The user must belong to a User Group that has permission to perform the *Delete SDS File* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot delete the file.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Delete SDS File" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

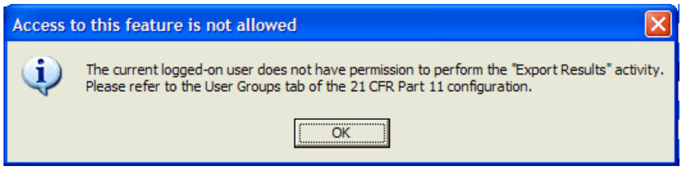
Export Results

The *Export Results* Controlled Activity controls the ability of users to export results for the User Runs, User Studies, and Templates File Types.

User Group Permission

The user must belong to a User Group that has permission to perform the *Export Results* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot export the results.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Export Results" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

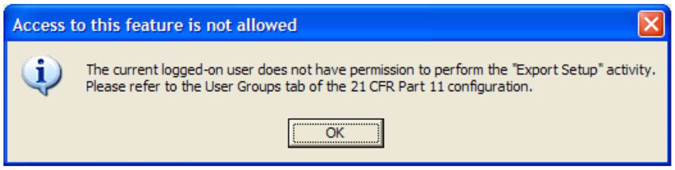
Export Setup

The *Export Setup* Controlled Activity controls the ability of users to export the plate setup information for the User Runs and Templates File Types.

User Group Permission

The user must belong to a User Group that has permission to perform the *Export Setup* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot export the plate setup information.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Export Setup" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

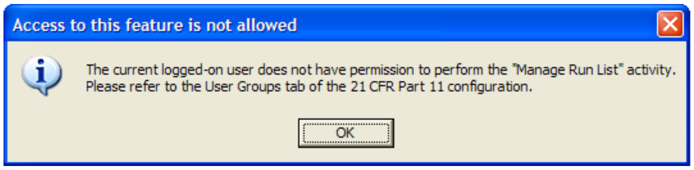
Manage Run List

The *Manage Run List* Controlled Activity controls access to the Run List Manager. Once in the Run List Manager, users can open, move, delete, and import the User Runs and User Studies File Types.

User Group Permission

The user must belong to a User Group that has permission to perform the *Manage Run List* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot open the Run List Manager.



Access to this feature is not allowed

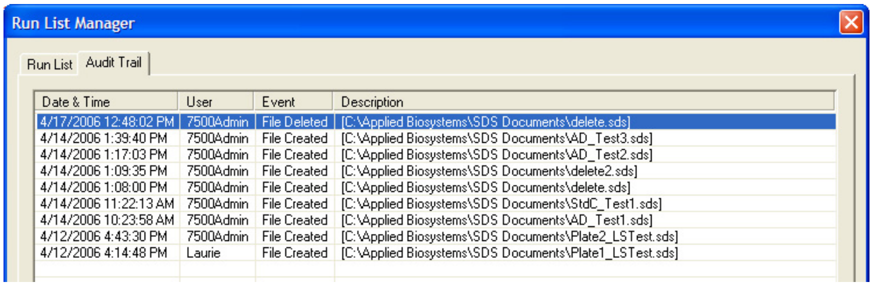
The current logged-on user does not have permission to perform the "Manage Run List" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Access Problems

Users who have access to the Run List Manager will not be able to open, move, delete, or import *.sds or *.sdm files in the following instances:

- They do not have access to the file location (that is, the user who created the file placed it in a location only he or she can access).
- The file has been deleted or moved using the Windows XP operating system.

IMPORTANT! The SDS Software does not track changes made to *.sds, *.sdm, or *.sdt files by the Windows XP operating system.



Run List Manager

Date & Time	User	Event	Description
4/17/2006 12:48:02 PM	7500Admin	File Deleted	[C:\Applied Biosystems\SDS Documents\delete.sds]
4/14/2006 1:39:40 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\AD_Test3.sds]
4/14/2006 1:17:03 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\AD_Test2.sds]
4/14/2006 1:09:35 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\delete2.sds]
4/14/2006 1:08:00 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\delete.sds]
4/14/2006 11:22:13 AM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\StdC_Test1.sds]
4/14/2006 10:23:58 AM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\AD_Test1.sds]
4/12/2006 4:43:30 PM	7500Admin	File Created	[C:\Applied Biosystems\SDS Documents\Plate2_LSTest.sds]
4/12/2006 4:14:48 PM	Laurie	File Created	[C:\Applied Biosystems\SDS Documents\Plate1_LSTest.sds]

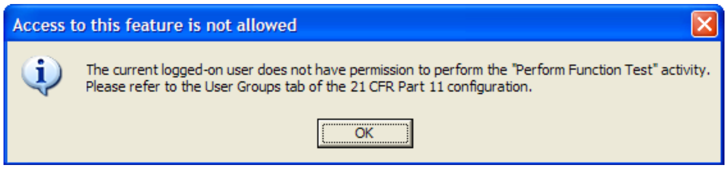
Perform Function Test

The *Perform Function Test* Controlled Activity controls the ability of users to perform functional tests on the Real-Time PCR System.

User Group Permission

The user must belong to a User Group that has permission to perform the *Perform Function Test* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot perform any functional tests.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Perform Function Test" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

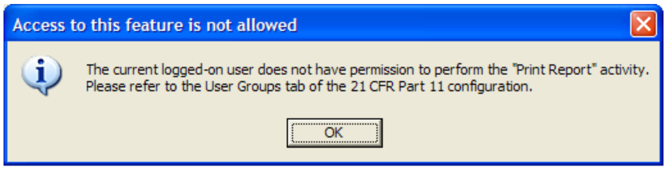
Print Report

The *Print Report* Controlled Activity controls the ability of users to print reports for the User Runs, User Studies, and Templates File Types.

User Group Permission

The user must belong to a User Group that has permission to perform the *Print Report* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot print any reports.


Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Print Report" activity. Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Notes

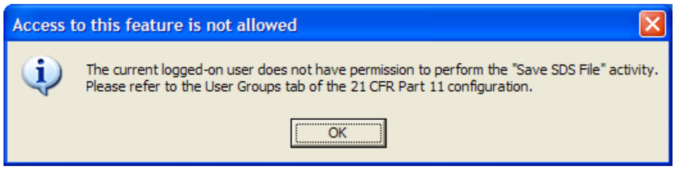
Save SDS File

The *Save SDS File* Controlled Activity controls the ability of users to save changes to the User Runs, User Studies, and Templates File Types. This includes both the **File ▸ Save** and **File ▸ Save As** functions.

User Group Permission

The user must belong to a User Group that has permission to perform the *Save SDS File* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot save the file.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Save SDS File" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

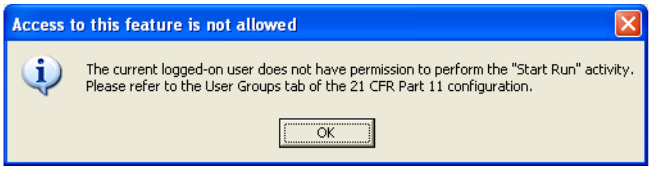
Start Run

The *Start Run* Controlled Activity controls the ability of users to start runs.

User Group Permission

The user must belong to a User Group that has permission to perform the *Start Run* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot start the run.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Start Run" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Notes

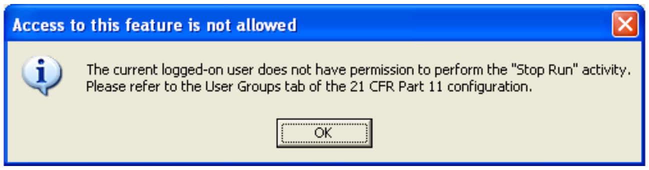
Stop Run

The *Stop Run* Controlled Activity controls the ability of users to stop runs.

User Group Permission

The user must belong to a User Group that has permission to perform the *Stop Run* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot stop the run.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "Stop Run" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

View Audit History

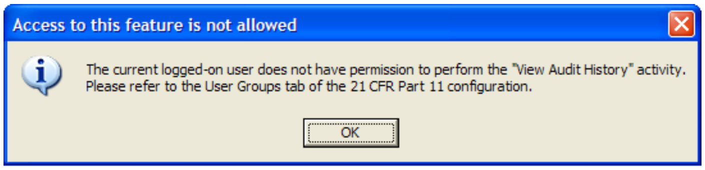
The *View Audit History* Controlled Activity controls the ability of users to view the audit trails within the SDS Software.

Note: For procedures on viewing and recording audit trails, see Chapter 5 on page 49.

User Group Permission

The user must belong to a User Group that has permission to perform the *View Audit History* Controlled Activity.

- If the user has permission, the SDS Software proceeds. No message or prompt is displayed.
- If the user does not have permission, the alert message below is displayed. The user cannot view the audit trail.



Access to this feature is not allowed

The current logged-on user does not have permission to perform the "View Audit History" activity.
Please refer to the User Groups tab of the 21 CFR Part 11 configuration.

Notes

Glossary

***.sdm file**

SDS Multi-Plate Document.

***.sds file**

SDS Document.

***.sdt file**

SDS Template.

21CFR11 module

See *21 CFR Part 11 module*.

21 CFR Part 11 module

An enhancement to SDS Software v1.4 that can be purchased separately. The 21 CFR Part 11 module can assist users in complying with FDA Title 21 Code of Federal Regulations Part 11, which regulates electronic records and electronic signatures.

authentication

A determination made by the SDS Software that a user has a valid user account, which is required to log in to the SDS Software. In order for the user account to be valid, it must be:

- Created in the Microsoft® Windows® XP operating system, *and*
- Be a member of at least one of the SDS Software User Groups.

Calibration Audit Trail

A data auditing record that displays the history of creations, deletions, or updates that occur in system calibration data collected from a 7500/7500 Fast instrument.

Configuration Audit Trail

A data auditing record that displays the history of creations, deletions, or updates that occur in system configuration data. This includes configuration data for the 21CFR11 module, system analysis parameters, and hardware.

Controlled Activity

A predefined operation in the SDS Software that users are either allowed to perform or prevented from performing (for example, *Configure System*).

data auditing

A feature of the 21CFR11 module that records changes (creations, deletions, and updates) over time for SDS File Types. The record of changes can be viewed in the SDS Software audit trails:

- Calibration Audit Trail
- Configuration Audit Trail
- Individual Audit Trail
- Run List Audit Trail

E-Signatures

1) Electronic signatures. An E-Signature is the electronic equivalent of a user's handwritten signature.

2) A feature of the 21CFR11 module that regulates E-Signatures for Signing Types predefined for the SDS File Types.

Event Log

A record that displays the history of System Audit Events that occur in the system files. There are three predefined System Audit Events:

- Failed login attempt
- Successful login
- Failed E-Signature attempt

FDA

Food and Drug Administration.

File Type

The file categories that occur within the SDS Software. The File Types discussed in this document are:

- User Runs, which are stored in SDS Documents (*.sds files).
- User Studies, which are stored in SDS Multi-Plate Documents (*.sdm files).
- Templates, which are stored in SDS Templates (*.sdt files).
- System Configuration.
- System Calibration.
- System Run List.

Individual Audit Trail

A data auditing record that displays the history of creations, deletions, or updates that occur in an *.sds, *.sdm, or *.sdt file.

legacy file

A file containing a User Run, User Study, or Template from an earlier version of the SDS Software. Data auditing and E-Signatures cannot be enabled for legacy files.

permission

The right to perform a particular Controlled Activity.

Run List Audit Trail

A data auditing record that displays the history of creations, deletions, or updates of the *.sds or *.sdm files that are included in the System Run List.

SDS

Sequence Detection System.

SDS Software

Sequence Detection System Software.

Signing Type

A predefined category in the SDS Software for which an E-Signature can be recorded. Each Signing Type has a defined meaning and associated data fields when applied to a specific File Type file.

For example, a user who records an E-Signature in an *.sds file for the Signing Type *Approval of Plate Setup*, is approving the current well and detector information for that *.sds file.

system

The SDS chemistry, consumables, instrument, and software.

System Run List

References to all User Runs and User Studies created in or imported into the SDS Software.

user

The individual running the SDS Software.

User Group A collection of user accounts managed by the Windows XP operating system. There are five User Groups that the SDS Software is programmed to recognize:

- SDS Administrators
- SDS Scientists
- SDS Technicians
- SDS Service
- SDS ESignature

wizard A software application that guides a user through a sequence of activities.

Index

Numerics

21CFR11 module
- and the Configure System Controlled Activity 74
- configurable features 3, 32
- configuring 11, 31
- configuring after installation 11
- definition 81
- features 2
- procedures required to install 9, 10
- registration code 10, 24

A

Analyze Data File 73

Applied Biosystems
- contacting viii
- customer feedback on documentation viii
- Information Development department viii
- Technical Support viii

assumptions for using this guide v

audit trails
- data auditing configuration 46
- recording changes 48
- viewing 49
- within the SDS Software 46

B

Best Practices 5

bold text, when to use v

C

Calibrate System 73

Calibration Audit Trail
- and configuring data auditing 38
- description 46
- viewing 52

CAUTION, description vi

compliance 4

configurable features 32
- data auditing 37
- E-Signatures 40
- idle timeout 33
- User Group permissions 35

Configuration Audit Trail
- description 46
- viewing 49

Configure System 74

Controlled Activities
- Analyze Data File 73
- and User Group permissions 35
- Calibrate System 73
- Configure System 74
- Create SDS File 74
- Delete SDS File 75
- Export Results 75
- Export Setup 76
- Manage Run List 77
- Perform Function Test 78
- predefined in the SDS Software 72
- Print Report 78
- Save SDS File 79
- Start Run 79
- Stop Run 80
- View Audit History 80

conventions
- bold text v
- for describing menu commands v
- IMPORTANT! vi
- in this guide v
- italic text v
- Notes vi
- user attention words vi

Create SDS File 74

customer feedback, on Applied Biosystems documents viii

D

data auditing
- and File Types 37
- Calibration Audit Trail 38
- configuring 37
- Individual Audit Trail 37
- Run List Audit Trail 38
- System Configuration data 32

Delete SDS File 75

documentation, related vii

domain 25

E

errors
- Save and Export functions 28

E-Signatures
- and data auditing 40
- and File Types 40
- and Signing Types 40
- configuration 60
- configuring 40
- ESignatures User Group 41
- recording 63
- restrictions for required E-Signatures 61
- viewing 66

E-Signatures tabs 41
- Calibration 69
- User Runs, User Studies, Templates 66

ESignatures User Group 41

Event Log
- description 46
- viewing 51

Export functions, errors 28

Export Results 75

Export Setup 76

F

FDA Title 21 Code of Federal Regulations Part 11
- compliance information 4
- FDA website 4
- regulation 2

FDA website 4

File Types
- and data auditing 37
- and E-Signatures 40
- definition 82
- discussed in this document 3
- Signing Types for 58, 61

H

Help system, accessing vii

I

idle timeout
- configuring 33
- value 34

Individual Audit Trail
- and configuring data auditing 37
- description 46
- recording changes in 48
- saved changes 37
- User Studies 38
- viewing 53

Information Development department, contacting viii

installation
- method 8
- required privileges 8
- using the Installation and Maintenance Guide 8
- using the Real-Time System Setup Wizard 8, 9

italic text, when to use v

L

logging in to the SDS Software 24

M

Manage Run List 77

menu commands, conventions for describing v

MSDSs, obtaining viii

multiple user accounts 27

O

online Help. *See* Help system

P

passwords 13

Perform Function Test 78

Print Report 78

R

Real-Time System Setup Wizard 8

registration code 10, 24

Run List Audit Trail
- and configuring data auditing 38
- description 46
- viewing 55

S

Save As Function 47

Save functions, errors 28

Save SDS File 79

SDS Software
- audit trails 46
- Controlled Activities 72
- installation method 8
- installing 7
- logging in 24
- Signing Types 58

Signing Types
- and E-Signatures 40
- associated data 58
- predefined in the SDS Software 58
- restrictions 61

Start Run 79

Stop Run 80

T

Technical Support, contacting viii

text conventions v

training, information on viii

U

user attention words, described vi

User Groups
- and Controlled Activities 35
- and the Windows XP operating system 12
- configuring permissions 35
- Controlled Activities 35
- creating 14
- creating after installation 9
- creating during installation 10

users
- adding to an existing User Group 18
- and the Windows XP operating system 12
- assigning to multiple User Groups 14, 18
- creating 12
- creating after installation 9
- creating during installation 10
- multiple user accounts 27
- passwords 13

V

View Audit History 80

W

WARNING, description vi

wizard. *See* Real-Time System Setup Wizard

Worldwide Sales and Support

Applied Biosystems vast distribution and service network, composed of highly trained support and applications personnel, reaches 150 countries on six continents. For sales office locations and technical support, please call our local office or refer to our Web site at **www.appliedbiosystems.com**.

Applied Biosystems is committed to providing the world's leading technology and information for life scientists.

Headquarters
850 Lincoln Centre Drive
Foster City, CA 94404 USA
Phone: +1 650.638.5800
Toll Free (In North America): +1 800.345.5224
Fax: +1 650.638.5884

06/2010

Applied Biosystems