User Bulletin

8200 Cellular Detection System Analysis Software v4.0

August 14, 2007

SUBJECT: 21 CFR Part 11 Software Console - Administrators Guide

In This User Bulletin

This user bulletin covers:

Introduction

The 21 CFR Part 11 console is a new feature of the Analysis Software v4.0 for the Applied Biosystems 8200 Cellular Detection System (CDS). The FDA Title 21 Code of Federal Regulations Part 11 regulates electronic records and electronic signatures. The console allows a customer to integrate the 8200 CDS in to the customer's 21 CFR Part 11 compliant workflow. The 8200 CDS with Analysis Software v4.0 is not validated as 21 CFR Part 11 compliant because Applied Biosystems did not perform system level testing of the 21 CFR Part 11 requirements.

IMPORTANT! Your company must ensure that all parts of the FDA regulation are followed. 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

The purpose of this guide is to describe the configuration and management tasks related to the 21 CFR Part 11 console.

The 21 CFR 11 console in 8200 CDS Analysis Software v4.0 provides useful security and monitoring features (Table 1)

Applied Biosystems

Table 1 8200 CDS Analysis Software v4.0 21 CFR 11 console features

Category	Features
Security	The security features prevent unauthorized access to the 8200 CDS Analysis 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 8200 CDS Analysis Software in the Event Log. • Verifying each user's permission to perform predefined Controlled Activities. • In the run file, detecting changes to data that have occurred while the 21 CFR Part 11 is enabled.
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 events. • When an E-Signature is *required* for an event, 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 8200 CDS Analysis Software data by: • Storing audit trails to independently record the date and time users create, delete, or update 8200 CDS 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 8200 Cellular Detection System. • Recording the instrument's serial number.

To customize the 21 CFR Part 11 console for your company, configure the console features as summarized in Table 2.

Table 2 Workflow summary for configuring the 21 CFR Part 11 console

Task	Software Location
Login as Administrator.	Analysis Software
Open the console.	Analysis Software ▸ Tools ▸ 21 CFR Part 11 ▸ Open 21 CFR Part 11
Define the scope of user and data auditing security.	21 CFR Part 11 console, Administrator Settings tab)
Specify the tasks to be audited and tasks to require E-Signature.	21 CFR Part 11 console, Audit and E-Sig tab
Set up user accounts for existing groups. For each user, enter the user name and assign a password and group(s).‡	21 CFR Part 11 console, User and Groups tab
(Optional) Create and assign users to new groups. ‡	21 CFR Part 11 console, User and Groups tab

‡ After installing the 8200 CDS Analysis Software v4.0, all users and groups created in 8200 CDS Analysis Software v3 must be re-created. To assign a user to a new group, first create the user group, then create or edit the user account.

To back up the configuration settings, groups, and users, go to Analysis Software ▸ Tools ▸ 21 CFR Part 11 ▸ Backup (for information see "Appendix A Configuring the Console Reference Guide" on page 9).

To copy configuration settings, groups, and users to additional computer(s), see "Copying Configuration Settings, Groups, and Users to Additional Computer(s)" on page 7.

Installation

Backup all data files to another location, then install the Analysis Software version 4.0 according to the instructions and installation wizard prompts.

IMPORTANT! During the installation process, the previous version of Analysis Software is removed, including the data files, users, and groups. Be sure to save the data back up file(s) to your network, USB device, or other safe site/media before beginning installation.

After installation is complete, delete the **AppliedBiosystems**/8200 Analysis Software folder. There is no space between “Applied” and “Biosystems”. The folder with a space, Applied Biosystems/8200 Analysis Software folder, contains the 8200 Analysis Software version 4.0 files.

To log in for the first time after installation:

1. Double-click the 8200 Analysis Software icon on the desktop. The login window is displayed.
2. Enter the default user name Administrator, the default password Administrator, and the default group Admin JT (Figure 1). The user name and password are case sensitive and must be capitalized.

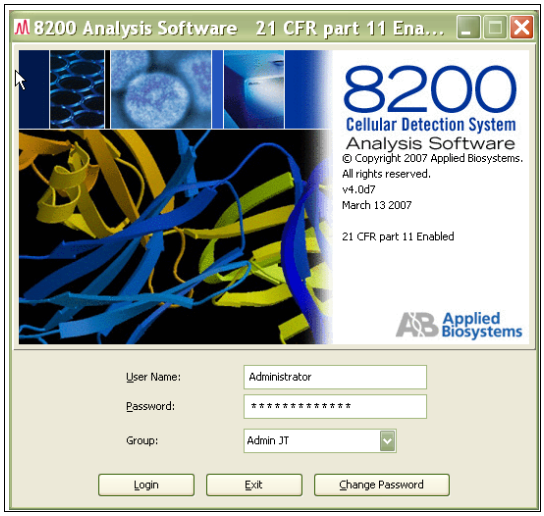

Figure 1 Accessing the 21 CFR Part 11 console

Applied Biosystems recommends that you change the default password immediately. To change the password, select **Change Password** and follow the directions that are displayed. The password can be 6 to 30 characters and can include a blank (excluding the first or last character) and other special characters, such as hyphens.

Accessing the Console:

1. Login using the Administrator user name, password, and group. The Analysis Software window (Figure 2) displays.

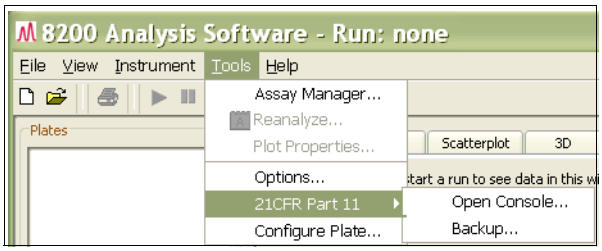

Figure 2 Excerpt of the Analysis Software window

2. From the Analysis Software file menu, select **Tools**, then 21 CFR Part 11, then **Open Console** (Figure 2). The console is displayed (Figure 3).

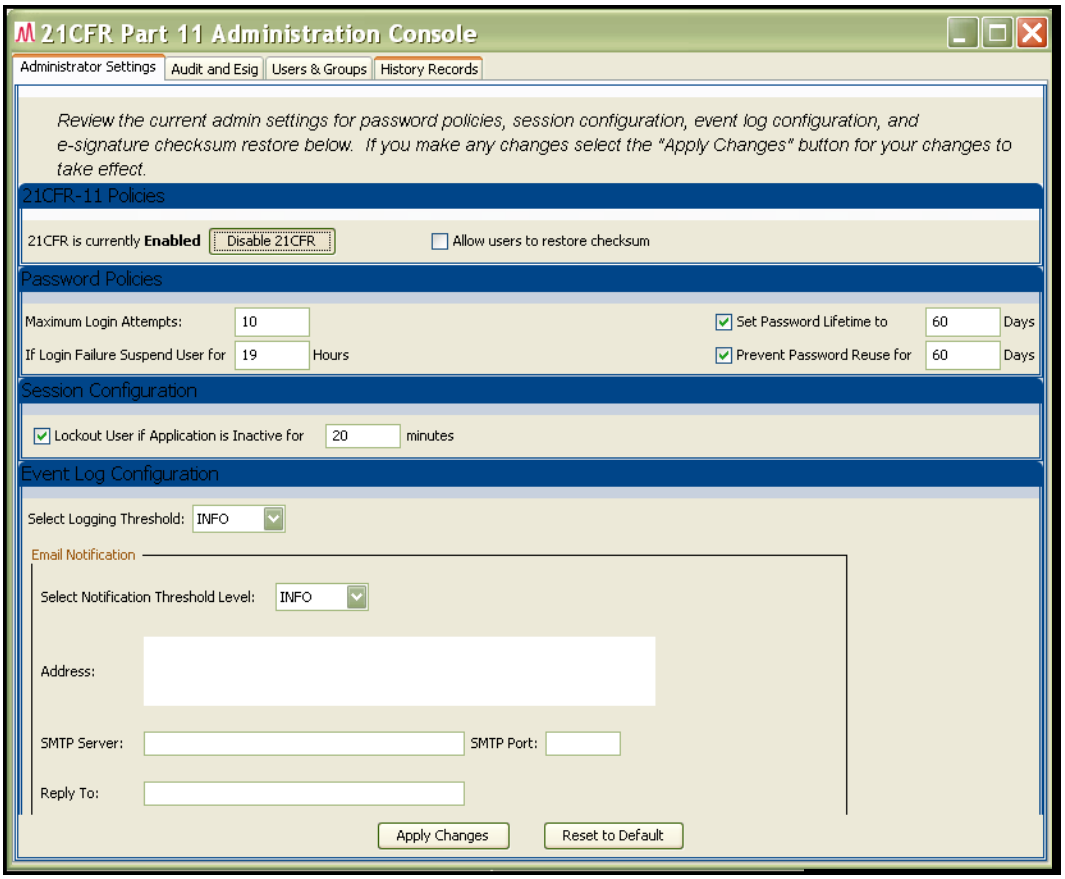

Figure 3 The 21 CFR Part 11 Console window

Configuring the Console

Configure Administrator and Audit and E-Sig Settings

For information, see "Define the Scope of User and Data Auditing Security" on page 9 and "Specify Audited and E-Signature Tasks" on page 10.

1. In the Administrator Settings tab, set the:
   - 21 CFR 11 Policies
   - Password Policies
   - Session Configuration
   - Event Log Configuration
2. Click **Apply Changes**.
3. Click the **Audit and E-Sig Settings** tab, then:
   - Select each item to audit and the corresponding setting
   - Select each item for E-Signature and, if necessary, overwrite or delete the corresponding meaning text.
   - If necessary, overwrite or delete the current E-Signature challenge text.

   When the tab window is closed, the information is saved.

Set Up User Accounts for Existing Groups

For information, see "Set Up User Accounts" on page 12.

1. In the Users and Groups tab, click **Users**. The Users window is displayed.
2. Set up user accounts for the existing groups (Admin JT, Default, R&D) by clicking **New User**, then, in the Create New User window:
   - Define the new user
   - Setup the password
   - Assign the group
3. Click **Save User**

Create and Assign Users to a New Group

For information, see "(Optional) Create New Groups" on page 14.

1. In the Users and Groups tab, click **Groups**. The Groups window is displayed.
2. Set up the new group by clicking **New Group**, then, in the Create New Group window:
   - Define the new group
   - Select permission(s) for the group
   - Select user(s) to assign to the group
3. Click **Save Group**.
4. To assign the group, create or edit the user account.

Backing Up the 21 CFR Part 11 Console Configuration Settings

To back up the 21 CFR Part 11 Console settings and the Auditing and E-Signature Events in the History Records:

1. Login to the 8200 CDS Analysis Software as Administrator.
2. From the Analysis Software file menu, select **Tools ▸ 21 CFR Part 11 ▸ Backup**.
3. In the dialog box, enter a backup file path and name (for example: C:\8200\backup02Aug2007).

   IMPORTANT! If a file with the same name exists, the previous data is overwritten.
4. Click **Save**. A directory containing three file folders and two files is created. The backup dialog box closes. Use a compression utility such as WinZip® to compress and group the files in to a single archive file.

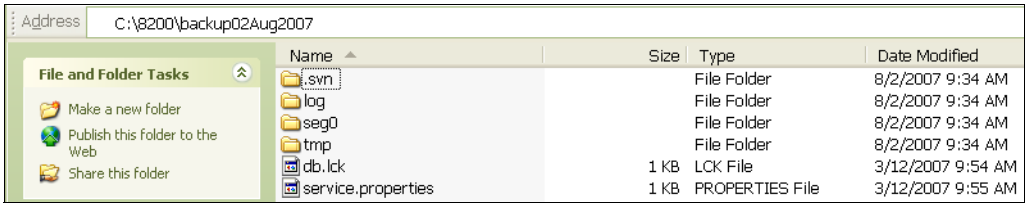

Figure 4 Contents of the backup folder

Copying Configuration Settings, Groups, and Users to Additional Computer(s)

To copy the 21 CFR Console configuration to other computers that have the 8200 CDS Analysis Software v4.0 software installed:

1. Back up the console (see "Appendix A Configuring the Console Reference Guide" on page 9) immediately after configuring the console. You can save the back up file to your network, USB device, or other safe site/media.
2. Exit the 8200 CDS Analysis Software.
3. On the additional computer, browse to C:\Program Files\Applied Biosystems\8200 Analysis V4.0 (or the folder where you installed the 8200 software).

4. Delete the folder named “IA”.

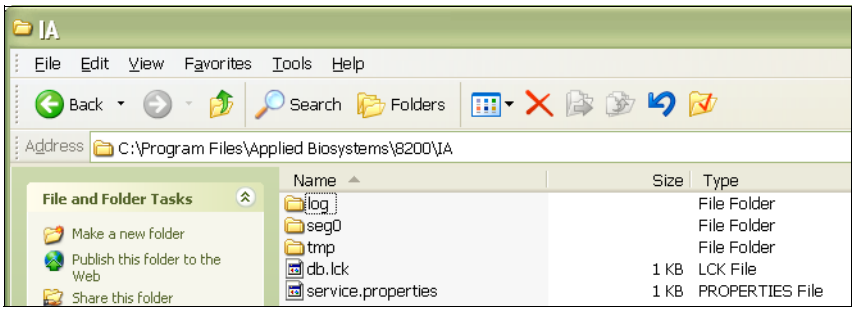

Figure 5 IA folder location and contents

5. Browse to the folder where you stored the backup file.
6. Copy the backup file to the C:\Program Files\Applied Biosystems\ 8200 Analysis V4.0 (or the folder where you installed the 8200 software).and rename the folder “IA”

IMPORTANT! When saving the 21 CFR Console configuration settings, all Auditing and E-Signature Events in History Records are saved also.

Appendix A Configuring the Console Reference Guide

Overview

Note: When reviewing your selection of tasks or permissions, such as an Enabled box, a check mark indicates that the task or activity is enabled (for example, selected or permitted). A blank box indicates that the item or activity is disabled or not permitted. See Figure 6 on page 10 and Figure 7 on page 12.
Similarly, a check mark in the category check box indicates all tasks or activities in the category are enabled. A blank category check box indicates all tasks or activities in the category are prohibited. A hyphen in the category check box indicates some tasks or activities in the category are enabled and some are disabled.

Define the Scope of User and Data Auditing Security

In the Administrator Settings tab (Figure 3 on page 5), make entries in the following sections:

- **21 CFR 11 Policies**
  - If necessary, enable the 21 CFR 11 utilities by clicking the Enabled button. The button changes to “Disable 21 CFR.”
  - (Optional) Click the “Allow users to restore checksum” check box to prevent opening a run file that has been altered without using the 8200 CDS Analysis Software (for example, copying data files in to the run file).

    The Checksum feature sums the data electronic bits, and stores the resulting value. The value is updated when a user closes a run file, opens or creates a run file, and exits the 8200 Analysis software. The next time data is accessed, the Checksum feature sums the data electronic bits and compares the result to the previous checksum value. If the sums match, the data is accepted as changed only through the 8200 CDS Analysis Software.

    If the sums are different, the 8200 CDS Analysis Software displays a failed validation message. If the user is permitted to restore checksum, the user can choose to update the checksum value and open the data file as fully accessible. If the checksum value is not updated, the file can be opened as read-only.
- **Password Policies** - Enter the number of times a user can enter an incorrect password (Maximum Logon Attempts field) before being locked out and the time frame of the lock out (If Login Failure Suspend User for “number of” hours) field.

  IMPORTANT! If you enter 0 in the Maximum Logon Attempts field, the user will never be locked out.

  Enter the maximum days a specific password can be used (Set Password Lifetime to “number of” Days), and the number of days before the password can be reused (Prevent Password Reuse for “number of” Days).
- **Session Configuration** - Set the amount of time a user can remain inactive (no mouse or keyboard activity) before the 8200 CDS Analysis Software automatically locks out access and requests re authentication.

  IMPORTANT! If you enter 0 minutes, the 8200 CDS Analysis Software will never time-out.

- **Event Log Configuration** - Select the logging threshold to set the type of records that are logged into the history file. The history file stores all records relating to global changes and all runs in Security Events, Audit Events, and E-Sig records.

  Note: Audit and E-Signature Events for an individual run are stored in the corresponding run number file. History file records are stored independent of the run file and are a compilation of events from all runs.

  To log:
  - No events, select **Off**. No history is saved.
  - Severe events (such as Login Failure Exceeding Max) only, select **Severe**.
  - Warnings (such as User Authentication Failure, Login Failure) and Severe events only select **Warning**.
  - Every event (such as User Authentication Success; all Warning and Severe Events), select **Info**.

See "Appendix A Configuring the Console Reference Guide" on page 9 for a list of events and the corresponding logging threshold.

Similarly, select the events that trigger email notification, then list the email addresses of the appropriate people to receive the notification. Your Information Technology (IT) group can supply the server and port information. Next enter the contact information to which the notified people can respond. Click **Test Email Configuration Settings** to send test emails to the addresses entered.

Click Apply Changes. The changes are saved. The window remains open.

Specify Audited and E-Signature Tasks

The Audit and E-Signature feature allows the administrator to select the activities to be tracked and actions that require E-Signature. Changes to your selections are automatically saved by the software.

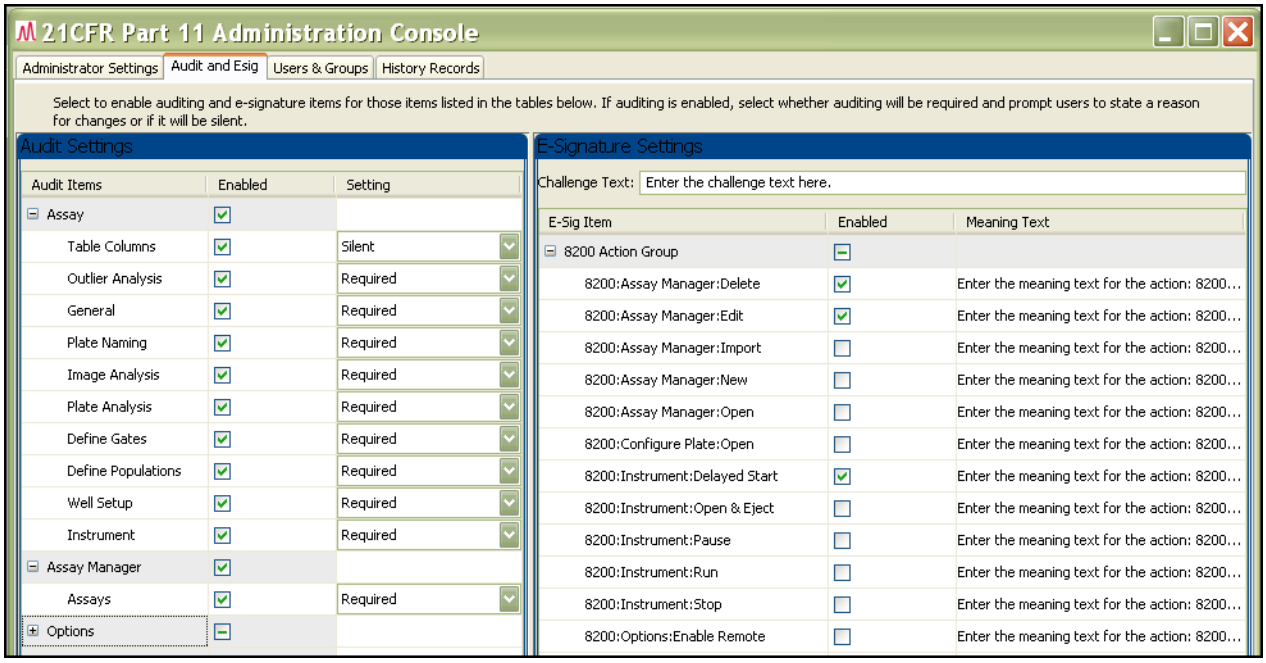

Figure 6 Audit and E-Sig tab

Audit Settings

In Audit Settings, click in the corresponding **Enabled** box to select each activity that will be tracked when the 21 CFR Part 11 console is enabled. A check mark indicates the activity is tracked. Select the guidelines for recording changes and a reason for change as defined in Table 3.

Note: Assay Manager tracks activities such as modifying, copying, deleting, or making additions to the assay file.

Table 3 Reason for Change configurations

Audit Item Configuration	Description	Audit Trail
Enabled and silent (Enabled box displays a check mark; setting box displays Silent.)	Saved changes are recorded when an enabled audit item is created, deleted, or updated. A Reason for Change Entry dialog box is never displayed.	All saved changes are recorded in the run file's Individual Audit Trail. Transactions are recorded for the life of the file.
Enabled, with Reason For Change Required (Enabled box displays a check mark; setting box displays Required.)	Saved changes are recorded when an enabled audit item is created, deleted, or updated. A Reason for Change Entry dialog box is displayed and the user may enter a reason for the change or close the dialog box.	
Disabled (Enabled box is blank; setting box displays Required or Silent)	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.

E-Signature Settings

In E-Signature Settings section, the text in the challenge text field displays in every E-Sig item dialog box. You can enter a statement such as "Your signature is required for 21 CFR Part 11 compliance," a legal statement, or a directive about an action the user may need to perform to return to their previous action.

Click in the corresponding **Enabled** box to select the activities that will be tracked by the software and require an E-Signature. Enter a message in the meaning text field that displays each time that item occurs, such as message explaining what the user is signing.

IMPORTANT! You must enter an appropriate message in order to conform to 21 CFR Part 11.

The default challenge or message text displays unless overwritten or deleted. The text you enter is saved when the dialog box is closed.

Set Up User Accounts

Set up an account for each user by completing the **Create New User** window in the Users and Groups tab User section (Figures 7 and 8).

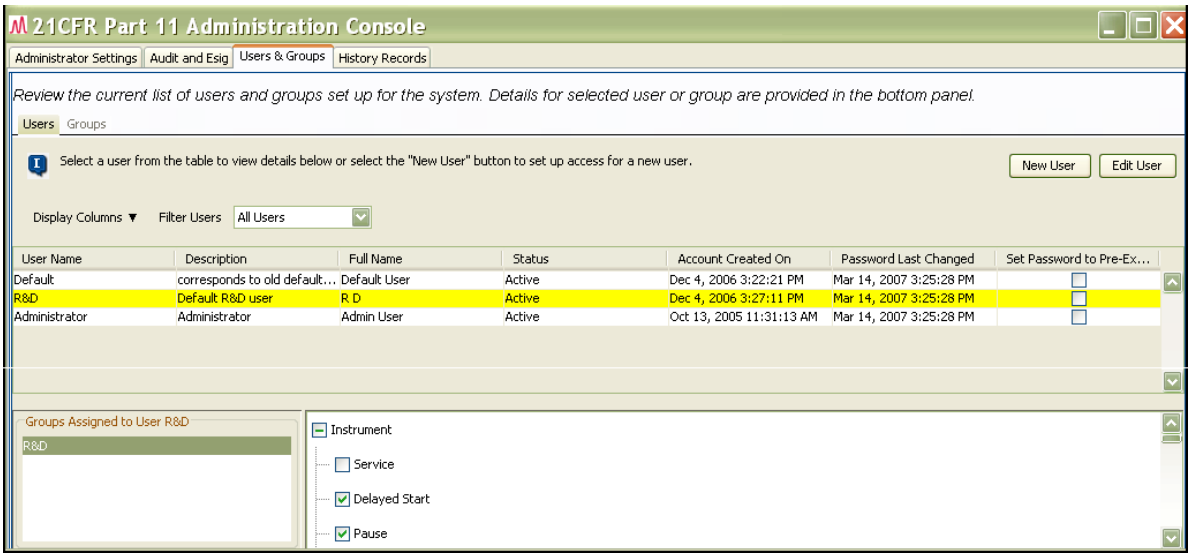

Figure 7 Users and Groups tab, Users section

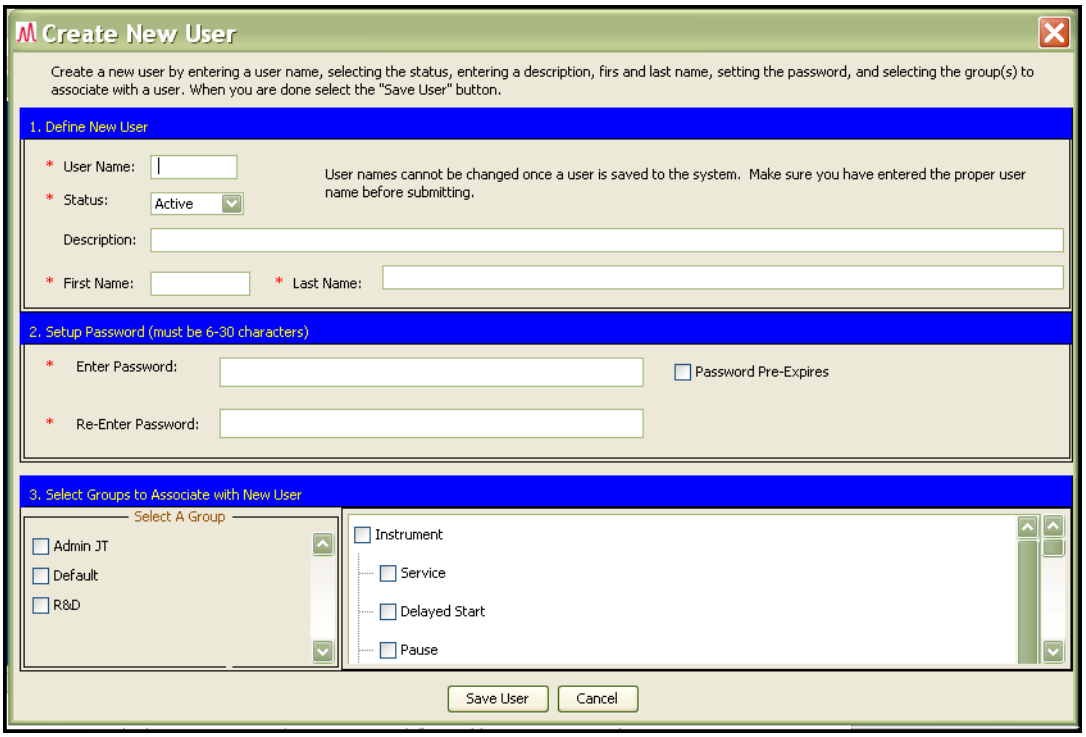

Figure 8 Create New User window

Create a New User Account

In the **Create New User** window, enter a User Name, assign Status, and enter First and Last Names. Be sure to enter the user name and first and last names accurately. Be aware that:

- The user name can be up to 30 characters and can include a blank (excluding the first or last character).
- User names can be retired, not deleted or changed after creation. Retired user names cannot be re-used. To be able to log in, a user name must be active.
- First and last names are required for recording E-Signatures. A blank first or last name prevents the user from recording E-Signatures.
- First and last name pairs can be re-used. A single user may have more than one user account on the same computer. For example, George W. Bush has one account with user name “BushG”, First name “George,” Last name “Bush”. Mr. Bush has a second account with user name “BushGW, First name “George,” Last name “Bush”.
- Several users may be using the same computer. For security, the Administrator may have one account for administrative purposes and one account for running the system.

Setup Password

A password is necessary for log in. A blank password prevents the user from logging in. The password can be 6 to 30 characters and can include a blank (excluding the first or last character). You can enter a default password. To ensure that the user changes the default password immediately, set the password to pre-expire. The user is required to change the password after logging in once with the default password.

The Password Lifetime (see “Define the Scope of User and Data Auditing Security” on page 9) ensures that the user changes the password on a regular basis.

Select Groups

Select the Group(s) the user can be associated with. A user can be assigned to multiple User Groups. When a group is selected, the permissions are displayed in the activities window. The permissions are displayed as read-only. To change permissions for the group, edit the group.

(Optional) Create New Groups

There are three predefined groups that assign the same permissions and exclusions to users:

- **Default** — Users are permitted to login only. They are prohibited from all activities. The user name/password at installation is Default/Default.
- **R&D** — Users are permitted to perform all activities except 21 CFR Part 11 console activities (for example, configuring the console or setting passwords and policies). The user name/password at installation is R&D/R&D.
- **Admin JT** — Administrator users are permitted to perform all activities. The user name/password at installation is Administrator/Administrator.

The Users and Groups ▸ Group feature (Figure 9 on page 14) allows the administrator to create user groups and specify the permitted 8200 CDS Analysis Software v4.0 controlled activities (see Figure 10 on page 15).

Note: The first time you configure User and Groups after installing the 8200 CDS Analysis Software v4.0, create all required groups first without assigning users. When completed, set up user accounts, then return to the group by clicking Users and Groups ▸ Group ▸ Edit Group. The users you created can then be selected and assigned to the group. Later, as new users are added to the system, you can set up the user account and assign the group in the **Create New User** window.

When creating a new group, be aware that:

- Users can be assigned to multiple User Groups.
- After logging in the 8200 CDS Analysis software with one of the User Groups to which a user belongs, the user is allowed to perform any activity that is permitted for that group.

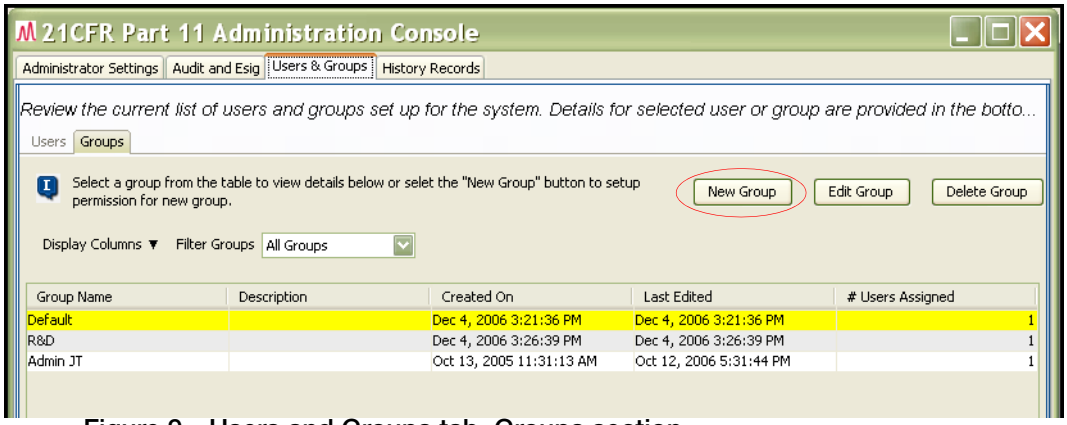

Figure 9 Users and Groups tab, Groups section

Create a New Group

1. In the Groups section, select **New Group** (Figure 9). The **Create New Group** window is displayed (Figure 10 on page 15).

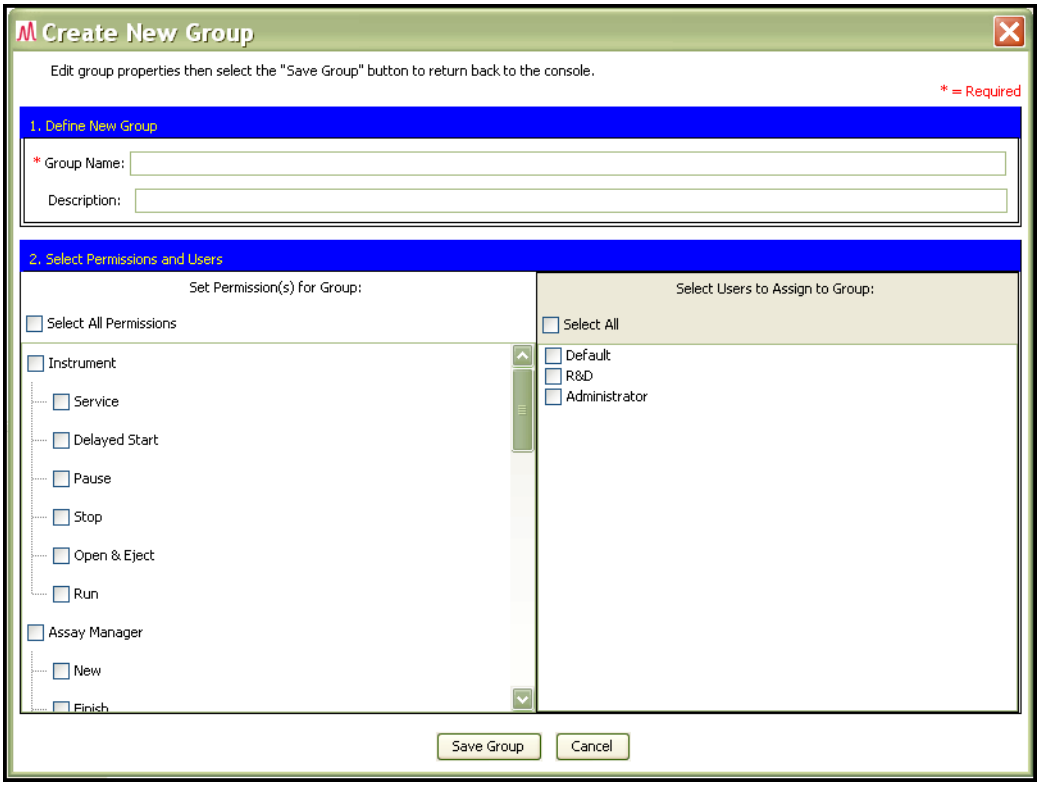

Figure 10 Create New Group window

2. Enter the **Group Name** and **Description**. The group name can not be changed after creation. The group name can be up to 30 characters and can include a blank (excluding the first or last character) and other special characters, such as hyphens. The description may be a list of privileges the user has as a member of the group.
3. Select Permissions by selecting the corresponding activity check box. A check mark is displayed. To allow all activities in *all* categories to be performed, select **Select All Permissions** check box.
4. (Optional) Select one or more of the predefined groups as assigned to the new group.
5. Click **Save Group**.

Appendix B History File Events by Logging Threshold Level

Table 4 Logging Threshold and Corresponding Events

Event Affecting:	Logging Threshold		
	Severe	**Warning‡**	**Info§**
• Checksum	NA	NA	Restore Checksum#
• 21 CFR 11	NA	NA	Change 21CFR11 Setting
• Login	Login Failure Exceeding Max	Login Failure	Login Success; Logout
• Password	NA	Change Password Failure	NA
• Password Expiry	NA	Max Grace Counts Exceeded‡‡	NA
• Session Configuration	NA	NA	Session Time-out
• E-Signature	E-Signature Failure Exceeding Max	E-Signature Authorization Failure	E-Signature Authorization Success
• User Authentication	NA	User Authentication Failure	User Authentication Success
• User Account	NA	Modify User Account	
• User Account	NA	Account State Change Failure§§	Create User Account

‡ In the **Event Log Configuration** dialog box**,** selecting **Warning** as the threshold displays all Warning and Severe Events

§ In the **Event Log Configuration** dialog box**,** selecting **Info** as the threshold displays all Info, Warning, and Severe Events

# Indicates the user selected to restore the checksum when opening the file.

‡‡After being notified that the password has expired, the user can two log in two more times with the expired password. After the two-login grace count is exceeded, this warning occurs at each log in attempt using the expired password.

§§The Administrator changed the status of the user account, for example, from suspended to retired.

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.

TRADEMARKS:

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

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

WinZip is a Registered Trademark of WinZip International LLC.

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

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**.

Applera is committed to providing the world's leading technology and information for life scientists. Applera Corporation consists of the Applied Biosystems and Celera Genomics businesses.

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

08/2007

Applied Biosystems

Part Number 4383718 Rev. B
Stock Number 113UB02-02