This document is provided to customers who have purchased SCIEX equipment to use in the operation of such SCIEX equipment. This document is copyright protected and any reproduction of this document or any part of this document is strictly prohibited, except as SCIEX may authorize in writing.

Software that may be described in this document is furnished under a license agreement. It is against the law to copy, modify, or distribute the software on any medium, except as specifically allowed in the license agreement. Furthermore, the license agreement may prohibit the software from being disassembled, reverse engineered, or decompiled for any purpose. Warranties are as stated therein.

 Portions of this document may make reference to other manufacturers and/or their products, which may contain parts whose names are registered as trademarks and/or function as trademarks of their respective owners. Any such use is intended only to designate those manufacturers' products as supplied by SCIEX for incorporation into its equipment and does not imply any right and/or license to use or permit others to use such manufacturers' and/or their product names as trademarks.

SCIEX warranties are limited to those express warranties provided at the time of sale or license of its products and are SCIEX's sole and exclusive representations, warranties, and obligations. SCIEX makes no other warranty of any kind whatsoever, expressed or implied, including without limitation, warranties of merchantability or fitness for a particular purpose, whether arising from a statute or otherwise in law or from a course of dealing or usage of trade, all of which are expressly disclaimed, and assumes no responsibility or contingent liability, including indirect or consequential damages, for any use by the purchaser or for any adverse circumstances arising therefrom.

For research use only. Not for use in diagnostic procedures.

AB Sciex is doing business as SCIEX.

The trademarks mentioned herein are the property of AB Sciex Pte. Ltd. or their respective owners.

AB SCIEX™ is being used under license.

© 2018 AB Sciex LLC
Contents

CHAPTER 1: Overviews, 5
System Administration Overview, 5
32 Karat Software System Administration Overview, 6
  Instrument Activity Log, 6
  Audit Trails, 6
  User Privileges, 7
  System Administrator, 7
  Instrument Administrator, 7
  Users, 7
  Projects, 9

CHAPTER 2: System Administration Options, 11
Managing the 32 Karat Software, 11
Enterprise Options for the CESI 8000 Software, 12
  Features of the Enterprise Options Dialog, 12
Workstation Options (optional), 14
Email Options (optional), 14
General Options (optional), 15
  Save All Analysis Results, 15
  Logging Options, 15
  Security Options, 15
Instrument Login, 16

CHAPTER 3: System Administration Wizard, 17
System Administration Wizards, 17
  Features of the Select Administration Wizards Window, 17
    User Wizard, 17
    Instrument Wizard, 17
    Project Wizard, 18
    Restart Selected Wizard When Finished, 18
User Wizard, 18
Instrument Wizard, 20
Project Wizard, 20
  Creating a New Project, 21
Assigning Users to a Project, 23
Changing a Project's Settings, 25
Remove Projects, 28

CHAPTER 4: Additional Features, 29
System Administration Report Utility, 29
Electronic Signature, 30
  Role Names, 31
  Number of Levels, 31
Electronic Signature Reasons, 31
  Modifying the Electronic Signature Reasons, 31
Global Options, 32
System Activity Log, 32
  Manual Entry, 33
Export, 34
Archive, 34
Purge, 34

CHAPTER 5: Example Administration Setup, 35
Laboratory Personnel, 35
Process Completion, 37

APPENDIX A: Worksheets, 39
User Privileges, 39
CHAPTER 1

Overviews

CAUTION

Prior to using the system, refer to the Safety Manual for detailed information on the safe use and operation of the system.

When the 32 Karat software is first installed, many of the security features available are enabled. This is done to facilitate the installation of a secure environment and provide a project-centered structure. With security enabled, the 32 Karat software recognizes projects and enables the CESI 8000 software to associate projects with defined instruments.

System Administration Overview

There are two points to keep in mind as you work through the process of setting up system security.

- Once the system administrator mode of the software has been activated, it can only be disabled by the system administrator. If the system administrator's ID or password is lost or forgotten, it may be impossible to access some features of the software.
- The security of the system is closely linked to the security of the operating system being used.

The security features of the 32 Karat software have been designed to facilitate compliance with the United States Food and Drug Administration regulation defined in Title 21 CFR Part 11. This regulation concerns electronic signatures and electronic records requirements. The information provided here does not contain all the information you need to know about compliance with this or any other regulation. Simply using this or any other software product is not sufficient to assure compliance. Your organization's regulatory department can provide you with specific information about the policies and procedures that you must follow to be in compliance. There are also many books and training classes available on this subject. You are urged to become familiar with the appropriate rules and regulations before setting up the security features of the 32 Karat software. You and your organization are ultimately responsible for regulatory compliance.
32 Karat Software System Administration Overview

There are multiple components to security. The availability of different features depends on how the system is configured. This section describes the components of system security in the 32 Karat software. The following section provides examples on how to set up your system.

Instrument Activity Log

The Instrument Activity Log is always on, even when the administration mode is not activated. A separate log exists for each instrument that is configured on the main window of the software.

For every user access of the instrument, the user, time, and activity is recorded. The system also records problem information from the hardware whether the user is present or not; this information is very useful in troubleshooting instrument issues. The Instrument Activity Log is not deleted when an instrument is deleted from the system, and it can be accessed even when the associated instrument no longer exists. If system administration has not been activated, the user is always recorded as System.

Over time, the Instrument Activity Log can become quite large. The software allows the user to archive the log and remove the original file. A special Log Viewer application is used to view the archived data. After a log is archived, the new Instrument Activity Log will indicate the date and location of the archive file.

Audit Trails

While the Instrument Activity Log tracks the usage of the hardware and the software, the Audit Trails track the history of data files and method files. The Data File Audit Trail is always active. Method File Audit Trails must be activated, but may be used in either administrator mode or standard mode.

Data File Audit Trail

A Data File Audit Trail records when the file was created, opened, or analyzed. Each time the data is analyzed a results section is created in the file; these results may be different depending on the method used for the analysis. The Data Audit Trail is used to track these changes, as well as keeping a record of when the file was accessed and by whom. A Data File Audit Trail remains with the data file even if the data file is moved to a different folder or renamed.

Method File Audit Trail

A Method File Audit Trail, when active, records all of the edits made to a method file. The changes that were made will be recorded, along with the user ID and the time the change occurred. Optionally, the user may be prompted to give a reason for the change. The Method File Audit Trail may be activated globally or for individual methods. Once activated for a method, it cannot be turned off. If a method is saved with a new name, a new Method Audit Trail will be created with the new method, and the old Method Audit Trail will remain with the original method.

Sequence Audit Trail

A Sequence File Audit Trail, when active, records all of the edits made to a sequence file. The changes that were made will be recorded, along with the user ID and the time the change
occurred. Optionally, the user may be prompted to give a reason for the change. The Sequence File Audit Trail may be activated globally or for individual methods. Once activated for a sequence, it cannot be turned off. If a sequence is saved with a new name, a new Sequence Audit Trail will be created with the new sequence, and the old Sequence Audit Trail will remain with the original sequence.

User Privileges

The 32 Karat software recognizes three classes of users: system administrators, instrument administrators, and general users. There may be more than one user of each type, and any individual can serve in more than one role. The default privileges of each user type are different. General users can be assigned unique privileges and security levels by the administrators.

The software may be started by anyone, and the main window displays. When System Administration mode is operating, any further actions will require a valid user name and password. That user name and password, and the privileges that have been assigned to it, will be in effect until the instrument or the software is closed.

System Administrator

The System Administrator has full access to the administration of the system. This is the individual who can establish new users, create and change passwords, assign users to projects, and assign privilege levels within those projects. The System Administrator can also establish the Instrument Administrator role; usually the System Administrator will also be an Instrument Administrator. There can be more than one System Administrator, and having a backup System Administrator is a good idea.

Be aware that when the System Administrator has logged in, anyone using the workstation may be able to obtain all privileges. The System Administrator should always log out of administration mode before leaving the workstation.

Instrument Administrator

The Instrument Administrator has far fewer privileges than the System Administrator. The Instrument Administrator can create a new instrument on the main page of the software, can modify the configuration of an instrument system, and can give or remove instrument access privileges to a user. The Instrument Administrator cannot create new users, or change the privilege levels of existing users; that is reserved for the System Administrator.

Be aware that when the Instrument Administrator has logged in, anyone using the workstation may be able to invoke Instrument Administrator privileges. The Instrument Administrator should always log out of administration mode before leaving the workstation.

Users

Users are individuals who may be assigned any or all of the privileges listed in the table below. They are assigned to one or more projects and one or more instruments (see below), and their
privileges can vary both between projects and between instruments. Users have no administrative privileges.

<table>
<thead>
<tr>
<th>Category</th>
<th>Selectable Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Open Data, Save Data, Properties (Description), Manual Integration Fixes</td>
</tr>
<tr>
<td>Electronic Signature</td>
<td>Sign Data Files, Multiple Files Sign, Multiple File Revoke</td>
</tr>
<tr>
<td>Sequences</td>
<td>Open Sequence, Save Sequence, Process, Properties, Summary, Custom Report</td>
</tr>
<tr>
<td>Control</td>
<td>Preview Run, Single Run, Sequence Run, Lock Instrument, Print Setup, Manual Control (Idle Only), Manual Control</td>
</tr>
<tr>
<td>Pretreatment</td>
<td>Open Pretreat, Save Pretreat, Properties</td>
</tr>
<tr>
<td>Advanced Report</td>
<td>Open Advanced Report, Save Advanced Report</td>
</tr>
</tbody>
</table>
Projects

In the 32 Karat software, a project is a way of organizing computer files and access privileges so that individual users cannot view or alter data and methods from projects to which they are not assigned. When a project is created, the System Administrator defines where the data files will be stored and who will have access to them. For each user who has access to a project, specific privileges can be defined which will only apply within that project. A given user may have different privileges in different projects.

NOTE Project security will not be complete unless Windows security features are activated.

There is one predefined project, named Default. All users have access to it at all times. The Default project should not be used for any analyses for which compliance is important. For optimum security, this project should be deleted. It should also be noted that, with one exception, the 32 Karat software does not allow data file names to be reused in a folder. This prevents the accidental over-writing of pre-existing data. The exception is if the word public is anywhere in the path name of the folder, such as C:\MyData\Public\MyProjectFiles. In this case, data in the folder MyProjectFiles can be overwritten without warning. In a secure system, the use of the word “public” in a path name should be avoided.

NOTE Additional information regarding system administration can be found in the manuals included with your system, and on the SCIEX web site.
CHAPTER 2
System Administration Options

When the 32 Karat software is launched, the Enterprise window displays. The Enterprise window is the main system module that controls many smaller applications, one of which is System Administration.

Managing the 32 Karat Software

System Administration is managed from the 32 Karat software Enterprise window. Once the Enable user logins and permissions feature is selected, the system administration functions will be activated. For more information see “General Features of the Enterprise Screen” within the CESI 8000 software online help.

There are two points to keep in mind as you work through the process of setting up system security.

- Once system administrator mode has been activated, it can only be disabled by the system administrator. If the system administrator's ID or password is lost or forgotten, it may be impossible to access some features of the software.
- The security of the system is closely linked to the security of the Microsoft Windows 7 Operating System.

Activating System Administration

1. From the Enterprise window, select Tools > Options. By default, System Administration Mode is selected in a new install.

2. When the Options window is displayed, select the Enterprise tab. For more information see Enterprise Options for the CESI 8000 Software.
Enterprise Options for the CESI 8000 Software

When the CESI 8000 software is first installed, the default setting disables the system administration login. Therefore, there is no need to log in when the CESI 8000 software is launched. When the **Enable user logins and permissions** option is selected, the system administration function is activated and security functions for login and project management are switched on. If this box is not selected, users are not required to login when accessing instrument or administration functions.

**NOTE** System administration should be enabled for security purposes. Once the system administrator mode of the software has been activated, it can only be disabled by the system administrator. If the system administrator’s ID or password is lost or forgotten, it may be impossible to access some features of the software.

Features of the Enterprise Options Dialog

**Obtain User Lists From**
There are two options for obtaining the user list:

- **Data System** - The list of users are maintained locally within the 32 Karat software. This choice is preferred for small organizations with few users. The software administrator will create the user names and access passwords. Users can be added or removed locally.

- **Domain Controller** - Requires that the 32 Karat software workstation be on a network. The list of potential users will be the list of users assigned to a particular network domain. In some large companies, this could be thousands of people, or it could be limited to the people in a single laboratory. It all depends on how the network is configured. When run under a domain controller, the user names and passwords will be those already assigned for that domain. Unless you are also the domain administrator, you will not be able to add and remove users yourself.

**IMPORTANT** If you select a domain on your network that is not under your control, you may lose access to the administrative features of the 32 Karat software, or you may not be able to use the software at all. In that case it will be necessary for the individual who has domain control to log in using their network password and assign administrative control of the 32 Karat software to you. If you cannot regain control, contact SCIEX Technical Support.

**Adding and Removing Users (Data System)**
When you add a new user to the data system. The User Information window displays and will prompt you for a User Name and Password.

Assign user privileges to users in the **CHAPTER 3, System Administration Wizards**. To delete a user, select the user name from the list, and select **Remove User**. Select **Change Password** to change the password for the selected user.

**Select domains to be scanned (Domain Controller)**
Select the domains to scan for users/groups. Select **Add Domain** to specify a domain to be added to the possible domains listed. Select **Remove** to delete a domain from the list. Selecting **Refresh** updates the list of current domains.
Allow passwords to be saved
When this option is selected, the user's password will be saved when the user logs into the system, and subsequent logins will not require the user to enter their password during this session of 32 Karat software activity (until the 32 Karat software is closed). This option is designed for systems where only one user will be using the workstation. Be aware that allowing passwords to be saved will decrease system security.

Enable single user login mode
When this option is selected, users can log in once and will not need to log in to each instrument individually.

Automatically login as the current domain user (Domain Controller)
When this option is selected, the current Windows user will be used for instrument login. If this is not selected, the user who logs onto the 32 Karat system will be used for all instruments. This option applies only for the domain controller.

Login Lockout (Domain Controller)
A system administrator can set up parameters for lockout of the system for specific users or after a given number of login attempts, when user logins and permission is enabled and the user list comes from a domain controller. Select Lockout Setup to view the options for setting up login lockout.

NOTE This locks out the 32 Karat software user accounts only, and does not affect Windows operating system access.

Lockout after bad logon attempts
Enter a number in this field. After this number of failed attempts to logon (bad password, etc.) the user attempting to logon will be locked out of the system. When this occurs, the user cannot access the system until the system administrator has unlocked their user account. Processes already started by the user (such as data acquisition) will not be affected. Entries will be made in the System Activity Log when a user is locked out.

Locked out users
Locked out users are listed in this area. To unlock a user, select the user or users, then select Unlock User.

Enable email notification
When this is selected, an email message will be sent to the designated addresses whenever a user is locked out. In order for the email notification to work, a MAPI or SMP-compatible email must be installed on the server and email notifications must be enabled on the Email tab of the Options dialog.

Message Text
The default message for email notification is User <USER> locked out of Data System on machine <MACHINE> due to failed login. This string is used for the subject line of the email generated. The subject line cannot be modified.

Enable user program
Select this option to launch a user program whenever a login lockout occurs. When the Enable user program option is selected, a UNC Universal Naming Conventions path to the program must be specified. The application will run on the enterprise machine.
User program
Enter the UNC Universal Naming Conventions path/filename for the user program to be launched.

Additional parameters
Enter any additional parameters required by the program here.

Workstation Options (optional)

The Workstation Options tab allows you to set status update options that apply to your workstation.

Status update interval
Instrument status can be displayed in the Enterprise window selecting View > Detail. When instrument status is displayed, the current status of each instrument is shown (i.e., Idle, Available, In Use).
Select how often the instrument status display is updated using this field.

Display the following warnings and confirmations?
To display a confirmation dialog when the 32 Karat software is closed, select this option.

Email Options (optional)

This tab is used to set up email options for your system.

Enable
Select this box to enable the settings for email. When unchecked, controls are disabled and previously-configured notifications are not sent by instruments.

SMTP
Select this option if SMTP is to be used for email.

Use this address in the ‘From’ field
Enter an email address of a valid user.

Mail server address
This field is used to specify the SMTP compliant email address of the local mail server to whom the email notification should be sent. This field can be a valid TCP/IP address or a URL name understood by the network.

Login Authentication
Select this option to provide a valid user name and password that may be required for SMTP.

SMTP Port
This field is used to specify the TCP/IP port number used for SMTP mail.

MAPI
Select this option if MAPI is to be used for email.
Profile
This field is used to specify the MAPI Profile to be used for sending email.

Test
Selecting this option will cause the system to attempt to connect to the email server and test the port (for SMTP) or will check if the profile exists on the server (for MAPI). This function will display a message box indicating the success or failure of the connection attempt.

General Options (optional)

Use this tab to turn on general enterprise options.

Save All Analysis Results
When this option is selected, every time an analysis is made on a data file, the results will be saved in the data file. If this box is not selected, only the original and most recent results will be saved in the file. If this box is selected, the results will be tagged with the user name and date of analysis. This makes it possible to open a specific result from the Open Data dialog, using the Open with Results option.

Logging Options
These options control how audit trail and activity logs are handled.

Automatically enable method audit trail
When this option is selected, the method audit trail will be enabled whenever a method is saved.

Automatically enable sequence audit trail
When this option is selected, the sequence audit trail will be enabled whenever a sequence is saved.

Activity log purge authorized only after archive
When this option is selected, the instrument activity log must be archived before it can be purged.

Enable system activity log
When this option is selected, the system activity log will be enabled. Once this is enabled, it cannot be turned off. It is recommended that you enable this log.

Security Options

Extended Security
When this option is selected, it causes a checksum to be calculated whenever a data file is closed. When the file is subsequently opened, its checksum is verified first. If the check fails (the calculated checksum for the file does not match the one previously calculated for the file) the
file cannot be opened, and an error is posted in the instrument activity log. Checksum verification is enterprise-wide.

**NOTE** Extended security does not affect security settings in non-networked environments (Stand-alone).

In addition, the Extended Security function provides additional security to the enterprise in the following ways.

- All system administrators have full access to everything.
- All non-system administrators will have read/execute rights to project directories for which they have rights.
- All non-system administrators will have read/write/execute rights to project subfolders for which they have rights.

This means that users in the project without system administrator rights will not be able to create subdirectories or files under the project directory, and they will not be able to rename or delete files under the project subfolders. Directories can still be created in project subfolders, but only through 32 Karat software.

**Log out Current User When Idle For**
When this option is selected, enter a number of minutes. If no mouse or keyboard activity is detected during the specified number of minutes in system administration mode, the system will:

- Cancel any open dialogs
- Cancel any Wizard in progress
- Log out of Administrative Mode

**Cancel an In-Progress Electronic Signature When Idle For**
If an electronic signature is in progress, it will be cancelled if there is no input for the specified number of minutes.

**Instrument Login**

Once users have been added to the data system and their privileges assigned to various instruments and projects in the database, they will be allowed to launch instruments to which they have been assigned.

When a user attempts to launch an instrument from the Enterprise window, they will be prompted to enter their user name, password and project to which they are logging in to.

All instrument logins are saved to the audit trail when it is enabled, and the system administrator may also set up additional security features to prevent unauthorized access to the system, see **Login Lockout (Domain Controller)**.
As the System Administrator, you can create projects, add users, and assign the user permissions. Projects are represented by assigned Windows folders that are recognized by the software. Access for each is set by the System Administrator.

**System Administration Wizards**

**IMPORTANT** The project and instrument name need to match in order to reflect what is shown in the CESI 8000 software. Do not use the special character “-” in the project or instrument name.

The System Administration Wizards allow you to easily manage the system administration functions within the 32 Karat software.

There are three different wizards available and each of these provide a pre-defined, step-by-step process to managing users and projects. The wizards are accessed from the 32 Karat software Enterprise window, select **Tools > System Administration Wizard.**

**Features of the Select Administration Wizards Window**

The 32 Karat software features three different System Administration Wizards.

**User Wizard**

- Use this wizard to assign system administration and/or instrument administration rights to users or groups defined on your system.
- Define the instruments and/or projects that are available to users or groups defined in the Enterprise window.
  
  For more information see **User Wizard.**

**Instrument Wizard**

- Use this wizard to assign user or group access to instruments/locations defined in the Enterprise window.
  
  For more information see **Instrument Wizard.**
**Project Wizard**

- Use this wizard to set up new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the Enterprise window.
- A project is comprised of a set of Windows directories for storage of Methods, Data, Sequences, and Templates, along with a project description.
- Using projects facilitates data management by ensuring related data are stored in designated directories that are consistent for all users.

For more information see Project Wizard.

**Restart Selected Wizard When Finished**

Select this box if you want to continue using the selected wizard (User, Instrument, or Project) after completing the current wizard task. For example, to set up multiple new projects without re-starting the Project Wizard.

**User Wizard**

The User Wizard is used to modify system access for users and groups, including:

- Assigning system administration rights to users or groups defined on the system.
- Assigning instrument administration rights to users or groups defined on the system.
- Defining the instruments and/or projects that are available to users or groups defined on the system.
- Adding or deleting users from the system (only for non-domain workstations).

1. Select **User** and select **Next** to proceed.

   NOTE Select the **Restart selected wizard when finished** option to add or edit more than one user. When selected, the user wizard will re-start when you select **Finish**, allowing you to add or edit additional users.

2. The Select User window displays.

   Select the user to modify and select **Next**.

3. Select **System Administration** to give this user full access to the system. This includes access to the User Wizard, Instrument Wizard, and Project Wizard.

   Select **Instrument Administration** to give this user access to the instrument systems only. This includes the ability to add, delete, and configure instruments.

   NOTE If neither box is checked, the user will have no access to system administration functions or instrument administration functions.

   When finished assigning privileges, select **Next** to proceed or **Finish** to exit the User Wizard.
4 From the list of instruments displayed in the Available Instruments frame, select the instruments for this user by double-clicking on the instrument or by selecting once to highlight the instrument and then selecting the green arrow to move it to the Selected Instruments frame.

**NOTE** If no instruments are displayed in the Available Instruments frame, expand the Enterprise icon by double-clicking locations until the desired instruments appear.

Assign all instruments within a laboratory or location to a user or group by selecting the entire location from the Available Instruments frame. When a location (for example, Enterprise) appears in the Selected Instruments frame, this means that all instruments in that location are selected.

When finished selecting instruments, select **Next** to proceed or **Finish** to exit the User Wizard.

5 From the list of projects displayed in the Available Projects frame, select the projects for this user by double-clicking on it or by selecting once to highlight the project and then selecting the green arrow to move it to the Selected Projects frame.

When finished selecting projects, select **Next** to proceed or **Finish** to exit the User Wizard.

6 The privileges displayed may be assigned as groups of items or as individual items. Select the items from those displayed in the Unassigned privileges frame and select the green arrow to move them to the Assigned privileges frame.

**NOTE** The Calibrate privilege enables the user to run a calibration sample to update the method calibration. In order to create or modify the calibration parameters in a method, the user must have the Save Method privilege assigned.

**NOTE** Select multiple projects or privileges by using **SHIFT** and **CTRL** and using the green arrow to assign them. Select a project or privilege and select **CTRL+ A** to select all projects or privileges.

When finished setting user privileges for each project, select **Next** to continue or select **Finish** to exit the User Wizard.

7 Select the level of signing authority that the user may have. A user may only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file.

**NOTE** Roles apply only when using domain security, not when using data system security.

When the electronic signature roles are defined for the user, select **Finish** to exit the User Wizard.
Instrument Wizard

The Instrument Wizard is used to assign a user or group access to instruments/locations defined in the 32 Karat software Enterprise window.

1. Select Instrument and select Next to proceed.

   NOTE Select Restart selected wizard when finished to add or edit more than one instrument or location. When selected, the Instrument Wizard will re-start when you select Finish, allowing you to add or edit additional instruments or locations.

2. Select the individual instrument or the location containing multiple instruments to which you want to assign a user or group access. Select Next to proceed.

3. The Select Users window displays.

   If you are selecting from data system users, select to highlight the name of the user you wish to add or modify. For more information on data system users see Enterprise Options for the CESI 8000 Software. Then select one of the green or red arrows to move the user to or from the instrument.

   If you are selecting users from a domain controller, select the domain from the drop-down list of domains available. (A domain is a functional portion of the network that has been set up by the Windows Domain Controller.) Once you have selected a domain, enter the user or group and select Check names to locate them within the domain. For more information on users from a domain controller see Enterprise Options for the CESI 8000 Software.

   • To select a group, select Groups and then enter the group name and select Check names to locate the group on the domain. Then select the valid group and select the green arrow to move the group to the instrument.

   • To select an individual user, select Users to enter a user name and locate the users within the domain and then select the green arrow to move the user to the instrument.

4. When finished selecting users, select Finish to exit the Instrument Wizard.

Project Wizard

The Project Wizard is used to set up new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the enterprise.

• A project is comprised of a set of Windows directories for storage of Methods, Data, Sequences, and Templates, along with a project description.

• Using projects facilitates data management by ensuring related data are stored in designated directories that are consistent for all users.
1. Select **Project** and select **Next** to proceed.

   **NOTE** Select **Restart selected wizard when finished** to add or edit more than one project. When selected, the Project Wizard will re-start when you select **Finish**, allowing you to add or edit additional projects.

2. The Select Project Action window will display. Select one of the options:
   - **Create a New Project** - Define a new project on the system, see **Creating a New Project**.
   - **Assign Users to a Project** - Assigns users or groups to existing projects in the system. This function can also be defined in the User Wizard.
   - **Change a Project’s Settings** - Edits or modifies an existing project in the system. This function can also be defined in the User Wizard.
   - **Remove Projects** - Removes a project from the system. When a project is removed using the wizard, access to the specified directories is removed. The actual data directories defined for the project are not deleted. Removal of data directories must be done by the Administrator (if desired) after proper backup has been performed.

   When you have made your selection, select **Next** to continue. See **Creating a New Project**, **Assigning Users to a Project**, **Changing a Project’s Settings**, or **Remove Projects**.

---

**Creating a New Project**

The Project Wizard is used to set up new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the enterprise.

1. Select **Create a new project** to define a new project on the system and select **Next** to proceed.

2. The General Project Settings window displays, where you will create the new project definition.

   Enter a descriptive **name** and define the **location** for the project. The project location can also be selected from available directories by selecting **File Open**. The location selected will automatically set up default directories for the project **Method**, **Data**, **Sequences**, **Templates**, **Pretreatments** (not used), and **Tune** (not used) directories.

   You may also enter a detailed text **description** for this project (optional).

   **NOTE** If you are entering paths manually, all paths must be entered using universal naming conventions. For example, `\ntserver\projects`.

   Once you have completed the project settings, select **Next** to continue or select **Finish** to exit the Project Wizard.

3. Select the audit trail to which the settings will apply, or select **All audit trails**.
In **Predefined audit trail reasons** define audit trail reasons that can be selected by users.

In **Reason to be added**, enter a reason and select **Add**. The list of defined reasons displays in the List of reasons field. To delete a reason, select the reason and then select **Delete**. To change the order of the reasons, select a reason then select **Move Up** or **Move Down**.

When **Automatically enable audit trail** is selected, the audit trail will automatically be enabled for all files of the specified type created in this project.

When **Prompt for reason at every change** is selected, you will be prompted for a reason whenever a change is made.

When **Prompt for reason when saving** is selected, you will be prompted for a reason for change only when a file is saved.

When **Do not prompt for reason** is selected, a prompt for reason will never be displayed.

When you have completed the audit trail settings, select **Next** to continue or **Finish** to exit the Project Wizard.

---

4. The electronic signature roles defined here specify the types of electronic signature roles that are applicable to this project. In one of the following steps, you will define specific electronic signature roles that each user assigned to this project will have.

The default names for the various **signature roles** are displayed, along with the signature reasons. Change a role name by highlighting it, then changing the role name.

Select the number of **signature levels** for this project. Default is 3. Once someone has electronically signed a data file, it may not be revoked by someone with a lower signature role.

The current signature reasons are displayed. To add, change, or delete Electronic Signature Reasons, select **Modify**.

---

5. From within the Modify Electronic Signature Reasons window add, change, or remove electronic signature reasons. To add a new reason, type it in the Reason to be added field and then select **Add**. To delete a reason, click on it to highlight it, then select **Delete**. Move a reason up or down in the list by highlighting it and then selecting the appropriate option.

When you have finished, select **OK** to save the new settings and return to the Define Electronic Signature Roles window.

---

6. When you have completed the project settings, select **Next** to continue to the Select Users window or select **Finish** to exit the Project Wizard.

If you have finished defining the roles, select **Next** to continue or select **Finish** to exit the Project Wizard.

---

7. If you are selecting from data system users, click on it to highlight the name of the user you wish to add or modify. For more information on data system users see Enterprise Options for the CESI 8000 Software.
If you are selecting users from a domain controller, select the domain from the drop-down list of domains available. (A domain is a functional portion of the network that has been set up by the Windows Domain Controller.) Once you have selected a domain, enter the user or group and select **Check names** to locate within the domain. For more information on users from a domain controller see **Enterprise Options for the CESI 8000 Software**.

- To select a group, select **Groups** and then enter the group name and select **Check names** to locate the group on the domain. Then select the valid group and select the green arrow to move the group to the project.
- To select an individual user, select **Users** to enter a user name and locate within the domain and then select the green arrow to move the user to the project.

**NOTE** If you plan to assign the same administration privileges, instrument privileges, and project privileges to all users in a group, it is faster to perform this function based on a Group selection, rather than assigning each user individually.

When finished selecting users, select **Next** to continue or select **Finish** to exit the Project Wizard.

---

8 The privileges displayed may be assigned as groups of items or as individual items. Select the items from those displayed in the Unassigned privileges frame and select the green arrow to move them to the Assigned privileges frame.

Privileges assigned from this location will apply to the entire project being created. Individual user privileges may then be later modified using the **User Wizard** interface.

**NOTE** The Calibrate privilege enables the user to run a calibration sample to update the method calibration. In order to create or modify the calibration parameters in a method, the user must have the Save Method privilege assigned.

When finished setting user privileges for the new project, select **Next** to continue or select **Finish** to exit the Project Wizard.

---

9 Select the level of signing authority that each user assigned to this project may have. A user may only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file.

**NOTE** Roles apply only when using domain security, not when using data system security.

If none of the users assigned to this project are assigned electronic signature roles for this project, a message will be displayed.

Once you have defined the electronic signature roles for each of the users, the new project is complete. Select **Finish** to exit the Project Wizard.

---

**Assigning Users to a Project**

The **Project Wizard** is used to set up new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the system.
1. Select **Assign users to a project** and select **Next** to proceed.

2. The Select Project window displays. Select the project to which you would like to assign users, and select **Next** to proceed.

3. The electronic signature roles defined here specify the types of electronic signature roles that are applicable to this project. In one of the following steps, you will define specific electronic signature roles that each user assigned to this project will have.

   The default names for the various **signature roles** are displayed, along with the signature reasons. Change a role name by highlighting it, then changing the role name.

   Select the number of **signature levels** for this project. Default is 3. Once someone has electronically signed a data file, it may not be revoked by someone with a lower signature role.

   The current **signature reasons** are displayed. To add, change, or delete Electronic Signature Reasons, select **Modify**.

4. In the Modify Electronic Signature Reasons window add, change, or remove electronic signature reasons. To add a new reason, type it in the Reason to be added field and then select **Add**. To delete a reason, click on it to highlight it, then select **Delete**. Move a reason up or down in the list by highlighting it and then selecting the appropriate option.

   When you have finished, select **OK** to save the new settings and return to the Define Electronic Signature Roles window.

5. When you have completed the project settings, select **Next** to continue to the Select Users window or select **Finish** to exit the Project Wizard.

   If you have finished defining the roles, select **Next** to continue or select **Finish** to exit the Project Wizard.

6. If you are selecting from data system users, click on it to highlight the name of the user you wish to add or modify. Then select one of the green or red arrows to move the user to or from the project. For more information on data system users see Enterprise Options for the CESI 8000 Software.

   If you are selecting users from a domain controller, select the domain from the drop-down list of domains available. (A domain is a functional portion of the network that has been set up by the Windows Domain Controller.) Once you have selected a domain, enter the user or group and select **Check names** to locate within the domain. For more information on users from a domain controller see Enterprise Options for the CESI 8000 Software.

   - To select a group, select **Groups** and then enter the group name and select **Check names** to locate the group on the domain. Then select the valid group and select the green arrow to move the group to the project.
• To select an individual user, select Users to enter a user name and locate within the domain and then select the green arrow to move the user to the project.

**NOTE** If you plan to assign the same administration privileges, instrument privileges, and project privileges to all users in a group, it is faster to perform this function based on a Group selection, rather than assigning each user individually.

When finished selecting users, select Next to continue or select Finish to exit the Project Wizard.

7 The privileges displayed may be assigned as groups of items or as individual items. Select the items from those displayed in the Unassigned privileges frame and select the green arrow to move them to the Assigned privileges frame.

Privileges assigned from this location will apply to the entire project being created. Individual user privileges may then be later modified using the User Wizard interface.

**NOTE** The Calibrate privilege enables the user to run a calibration sample to update the method calibration. In order to create or modify the calibration parameters in a method, the user must have the Save Method privilege assigned.

When finished setting user privileges for the new project, select Next to continue or select Finish to exit the Project Wizard.

8 Select the level of signing authority that each user assigned to this project may have. A user may only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file.

**NOTE** Roles apply only when using domain security, not when using data system security.

If none of the users assigned to this project are assigned electronic signature roles for this project, a message displays stating that.

9 Once you have defined the electronic signature roles for each of the users, the new project settings are complete. Select Finish to exit the Project Wizard.

### Changing a Project’s Settings

The Project Wizard is used to set up new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the enterprise.

1 Select Change a project’s settings and select Next to proceed.

2 The Select Project window displays. Select the project to which you would like to assign users, and select Next to proceed.
3 The General Project Settings window displays.
When changing a project’s settings, you cannot change the project name or file locations. 
This window allows you to enter or modify the text description (optional) for the selected project.
When you have finished, select Next to continue or select Finish to exit the Project Wizard.

4 Select the audit trail to which the settings will apply, or select All audit trails.
In Predefined audit trail reasons define audit trail reasons that can be selected by users.
In Reason to be added, enter a reason and select Add. The list of defined reasons displays in
the List of reasons field. To delete a reason, select the reason and then select Delete. To
change the order of the reasons, select a reason then select Move Up or Move Down.
When Automatically enable audit trail is selected, the audit trail will automatically be
enabled for all files of the specified type created in this project.
When Prompt for reason at every change is selected, you will be prompted for a reason
whenever a change is made.
When Prompt for reason when saving is selected, you will be prompted for a reason for
change only when a file is saved.
When Do not prompt for reason is selected, a prompt for reason will never be displayed.
When you have completed the audit trail settings, select Next to continue or Finish to exit
the Project Wizard.

5 The electronic signature roles defined here specify the types of electronic signature roles
that are applicable to this project. In one of the following steps, you will define specific
electronic signature roles that each user assigned to this project will have.
The default names for the various signature roles are displayed, along with the signature
reasons. Change a role name by highlighting it, then changing the role name.
Select the number of signature levels for this project. Default is 3. Once someone has
electronically signed a data file, it may not be revoked by someone with a lower signature
role.
The current signature reasons are displayed. To add, change, or delete Electronic Signature
Reasons, select Modify. The window shown below displays.

6 From the Modify Electronic Signature Reasons dialog, add, change, or remove electronic
signature reasons. To add a new reason, type it in the Reason to be added field and then
select Add. To delete a reason, click on it to highlight it, then select Delete. Move a reason up
or down in the list by highlighting it and then selecting the appropriate option.
When you have finished, select OK to save the new settings and return to the Define
Electronic Signature Roles window.
When you have completed the project settings, select **Next** to continue to the Select Users window or select **Finish** to exit the Project Wizard.

If you have finished defining the roles, select **Next** to continue or select **Finish** to exit the Project Wizard.

If you are selecting from data system users, click to highlight the name of the user you wish to add or modify. For more information on data system users see [Enterprise Options for the CESI 8000 Software](#).

If you are selecting users from a domain controller, select the domain from the drop-down list of domains available. (A domain is a functional portion of the network that has been set up by the Windows Domain Controller.) Once you have selected a domain, enter the user or group and select **Check names** to locate within the domain. For more information on users from a domain controller see [Enterprise Options for the CESI 8000 Software](#).

- To select a group, select **Groups** and then enter the group name and select **Check names** to locate the group on the domain. Then select the valid group and select the green arrow to move the group to the project.
- To select an individual user, select **Users** to enter a user name and locate within the domain and then select the green arrow to move the user to the project.

**NOTE** If you plan to assign the same administration privileges, instrument privileges, and project privileges to all users in a group, it is faster to perform this function based on a Group selection, rather than assigning each user individually.

When finished selecting users, select **Next** to continue or select **Finish** to exit the Project Wizard.

The privileges displayed may be assigned as groups of items or as individual items. Select the items from those displayed in the Unassigned privileges frame and select the green arrow to move them to the Assigned privileges frame.

Privileges assigned from this location will apply to the entire project being created. Individual user privileges may then be later modified using the **User Wizard** interface.

**NOTE** The Calibrate privilege enables the user to run a calibration sample to update the method calibration. In order to create or modify the calibration parameters in a method, the user must have the Save Method privilege assigned.

When finished setting user privileges for the new project, select **Next** to continue or select **Finish** to exit the Project Wizard.

Select the level of signing authority that each user assigned to this project may have. A user may only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file.

**NOTE** Roles apply only when using domain security, not when using data system security.
If none of the users assigned to this project are assigned electronic signature roles for this project, a message displays stating that.

11 When you have defined the electronic signature roles for each of the users, the new project settings are complete. select Finish to exit the Project Wizard.

Remove Projects

The Project Wizard is used to set up new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the enterprise.

1 Select Remove projects and select Next to proceed.

2 The Select Project window displays. Select the project you would like to remove and select Finish.

3 The selected project will be removed from the system.

NOTE When a project is removed using the wizard, access to the specified directories is removed. The actual data directories defined for the project are not deleted. If desired, removal of data directories must be done by an Administrator after a proper backup has been performed.
The System Administrator also has the ability of producing reports for various user aspects of the CESI 8000 Plus system, setting up electronic signature features, assign global security settings to the system, and establishing a system activity log.

**System Administration Report Utility**

The CESI 8000 software, which includes the 32 Karat software, incorporates a system administration report utility. This utility allows you to display the configuration for project settings, users and permissions, instrument configurations, and enterprise-wide settings. See Figure 4.1.

**Figure 4.1  System Administration Report Utility**

![System Administration Report Utility](image)
Electronic Signature

Electronic Signature features are set by the System Administrator and allow the user to acquire, review and/or sign off on data in a non-paper format.

The 32 Karat software includes technical controls to facilitate 21 CFR part 11 compliance. Activation of Electronic Signatures assists with this compliance process by allowing for the generation of electronic audit trails in addition to electronic record keeping.

1. Select System Administration Wizard from the Tools menu.

2. Select Project, then select Next.

3. Select Change a project’s settings, then select Next.

4. Select the project, then select Next.

5. Select Next, modify audit trail settings, then select Next.

6. Define the Electronic Signature Roles applicable to the selected project. Select Finish or Next to modify any other settings for the project.

Figure 4.2 Electronic Signature Roles Dialog
Role Names

Default names for the various signature roles are displayed, along with the signature reasons. To change a role name, highlight the role name, then retype it.

Number of Levels

Select the number of signature levels for this project. The default is 3. Once a user has electronically signed a data file, it may not be revoked by someone with a lower signature role.

Electronic Signature Reasons

Current signature reasons are displayed. To add, change, or delete Electronic Signature Reasons, click Modify.

Modifying the Electronic Signature Reasons

Use this dialog to add, change, or remove electronic signature reasons.

Type a new reason in the **Reason to be added** field, then click Add. To delete a reason, click on it to highlight it, then click Delete. To move a reason up or down in the list, highlight it, then select the appropriate directional button.

*Figure 4.3  Modify Electronic Signature Reasons Dialog*
Global Options

Select **Tools > Options > General Tab.** This option allows the System Administrator to automatically assign security settings to the entire system.

**NOTE** We recommend that you enable **Extended security** and select **Enable system activity log.**

**Figure 4.4** Enable System Activity Log and Extended Security

System Activity Log

1. To view the current system activity log, go to the **Main** Menu.

2. Select **File > System Activity Log > Display Log.**
   The current system activity log displays. Right-click in the table for a menu used to access the functions of the Activity Log.

   **IMPORTANT** This menu is disabled unless the user has System Administration or Instrument Administration rights assigned.
**Figure 4.5** System Activity Log Menu Options

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Detail</td>
<td>Displays details for the currently selected entry.</td>
</tr>
<tr>
<td>Manual Entry</td>
<td>Places a manual entry into the log.</td>
</tr>
<tr>
<td>Export</td>
<td>Exports the log or selected range of the log to a specific file.</td>
</tr>
<tr>
<td>Archive</td>
<td>Views the archived file.</td>
</tr>
<tr>
<td>Purge</td>
<td>Purges the system activity log.</td>
</tr>
</tbody>
</table>

**Manual Entry**

1. Place a manual entry into the system activity log.

2. Enter the information as necessary and click **OK**.

**Figure 4.6** System Activity Manual Entry Dialog
Export

Export the system activity log to a specified external file. Click **Save** to save the system activity log for the range selected in the file specified.

**Table 4.2 Menu Item Descriptions of Exported Activity Log**

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Enter the name to be used to store the system activity export file.</td>
</tr>
<tr>
<td>Save as type</td>
<td>Select the type of file to be saved.</td>
</tr>
<tr>
<td>Select record ranges</td>
<td>Select the option next to the desired range.</td>
</tr>
</tbody>
</table>

Archive

To archive the System Activity Log, select **File > System Activity Log > Archive** from the **Main** menu. A dialog opens so you can select the location for the archive file. A default name is assigned, with the .logarc extension. This file can be viewed using the Log Viewer which can be launched from: `C:\32Karat\LogViewer.exe`.

Purge

To purge the System Activity Log, select **File > System Activity Log > Purge** from the **Main** menu.

- If the **Activity Log Purge authorized only after archive** option is selected, the System Activity Log Archive dialog appears first. If confirmed, then the log is purged; otherwise, the purge operation is aborted.

  **NOTE** The user must have System Administration rights to use this command. The purge activity varies based on the global options selected. To view, select **Tools > Options > General Tab**.

- If the **Activity Log Purge authorized only after archive** box is not selected, then a confirmation message appears. If the user confirms, the purge operation occurs.

After the log is purged, an entry is added to the System Activity Log recording that the purge occurred.
In this section, a hypothetical lab is described. To suit the needs of this lab, various System Administration features are enabled. Use the User Project Privilege Worksheet in APPENDIX A, Worksheets to help organize the system.

**Laboratory Personnel**

Consider a small pharmaceutical laboratory with 3 employees consisting of a Manager, a Technician, and an Equipment Maintenance person named as follows:

Laboratory Manager - **LabMgr**

Laboratory Technician - **Tech**

Equipment Maintenance - **InstAd**

In this laboratory, various analyses of proteins, nucleic acids, and small molecules are performed. The laboratory manager has spent a great deal of time developing and validating a number of protein methods. The laboratory technician will begin using these methods while the laboratory manager continues development on new methods. The equipment maintenance person performs daily performance qualification on the instrument and system maintenance as required.

The laboratory manager sets up the System Administration as follows:

**Data System Users**

The following users will be added to the data system:

- LabMgr - System Administrator
- InstAd - Instrument Administrator
- Tech - Standard User

See Assigning Users to a Project in CHAPTER 3, System Administration Wizard for setup instructions.
System Projects
The lab manager will create the following projects:

- Protein
- Nucleic Acid
- Small Molecules
- Performance

See Creating a New Project in CHAPTER 3, System Administration Wizard for setup instructions.

Project Access
The lab manager will grant project access as follows:

- LabMgr - Protein, Nucleic Acid, Small Molecules, Performance
- InstAd - Performance
- Tech - Protein

See Assigning Users to a Project in CHAPTER 3, System Administration Wizard for setup instructions.

Signature Authority
The following signature authority is granted:

- LabMgr - Lab Manager on all projects, all permissions
- InstAd - Technician on Performance project, all permissions
- Tech - Technician on Protein project, all permissions

See Electronic Signature in CHAPTER 4, Additional Features for setup instructions.

System Instruments
The Instrument Administrator creates the following instruments:

- Protein - LabMgr, InstAd, and Tech as users
- Development - LabMgr and InstAd as user
- Performance - InstAd as user

See “CESI 8000 Instrument Configuration” within the Configuration section of the CESI 8000 software online help.

Adding a New User
At this point, the Lab Manager decides to hire a Bio-Statistician. Among other responsibilities, this employee will review data acquired by the Technician prior to submission to the manager for approval.

The System Administrator would modify the Protein Project as follows:

1. LabMgr selects Enterprise login from the Tools menu and enters the appropriate user name and password.
2 LabMgr selects **Options** from the **Tools** menu. The Analyst User is added at the **Enterprise Tab**.

3 LabMgr launches the System Administration Wizard from the **Tools** menu.

4 LabMgr uses the Project Wizard to modify the Protein project. The Shift Supervisor role name is changed to Analyst. The Analyst user is granted all Protein project permissions except for the control features.

The Electronic Signature Roles are as follows:

- LabMgr - Lab Manager on all projects
- InstAd - Technician on Performance project
- Tech - Technician on Protein project
- Analyst on Protein project

**Process Completion**

When the changes are complete, the Lab Manager selects **Enterprise Logout**. This example demonstrates how System Administration can be used in a laboratory setting.

Use copies of the worksheets in **APPENDIX A, Worksheets** to help plan the System Administration settings that are most appropriate for your laboratory.
## User Privileges

<table>
<thead>
<tr>
<th>Project Name</th>
<th>User</th>
<th>User</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Methods</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Method</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save Method</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instrument Setup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration Events</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peaks/Groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Suitability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review Calibration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calibrate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties (Description)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual Integration Fixes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Signature</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sign Data Files</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple File Sign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple File Revoke</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Name</td>
<td>User</td>
<td>User</td>
<td>User</td>
</tr>
<tr>
<td>--------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
</tbody>
</table>

### Sequences
- Open Sequence
- Save Sequence
- Process
- Properties
- Summary
- Custom Report

### Control
- Preview Run
- Single Run
- Sequence Run
- Lock Instrument
- Print Setup
- Manual Control (Idle Only)
- Manual Control

### Pretreatment
- Open Pretreat
- Save Pretreat
- Properties

### Advanced Reports
- Open Advanced Report
- Save Advanced Report

### Instrument Activity Log
- Purge Activity Log

### Security
- Access Common Folder

### Tune
- Open Tune
- Save Tune
- Properties
- Auto Tune
- Calibration

### Notes

---

Worksheets

CESI 8000 Plus High Performance Separation-ESI Module

System Administration Guide

RUO-IDV-05-3898-C | B11951AD
<table>
<thead>
<tr>
<th>User</th>
<th>Instrument Administrator</th>
<th>System Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instrument</th>
<th>User</th>
<th>User</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>