The Power of Precision

P/ACE MDQ Plus Capillary Electrophoresis System

System Administration Guide

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 the sole and exclusive representations, warranties, and obligations of SCIEX. 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.

(GEN-IDV-09-10816-D)

For Research Use Only. Not for use in Diagnostic Procedures.

Trademarks and/or registered trademarks mentioned herein, including associated logos, are the property of AB Sciex Pte. Ltd., or their respective owners, in the United States and/or certain other countries (see sciex.com/trademarks).

AB Sciex™ is being used under license.

EC REP

Leica Microsystems CMS GmbH
Ernst-Leitz-Strasse 17-37
35578 Wetzlar
Germany

🏭

AB Sciex Pte. Ltd.
Blk33, #04-06 Marsiling Industrial Estate Road 3
Woodlands Central Industrial Estate, Singapore 739256

Contents

Overview 1

Note: For regulatory and safety information for the capillary electrophoresis system, refer to the document: *Safety Notices*, *System Overview*, or *Operator Guide*.

This guide describes how to configure the 32 Karat software. The system administration features lets system administrators manage users, projects, and instruments. System administrators can also configure requirements for audit trails and electronic signatures.

In the 32 Karat software, an instrument is a software representation of a configuration of a P/ACE MDQ Plus system. It includes the detector, the tray configuration, and whether options for system suitability, Caesar integration, and qualitative analysis are available. If more than one detector is available, then we recommend creating at least one instrument for each detector.

After the software is installed, many of the security features available are enabled, which facilitates the installation of a secure environment and provide a project-centered structure.

The 32 Karat software provides a secure user environment, which supports the 21 CFR Part 11 compliance for the creation of electronic records, with the implementation of:

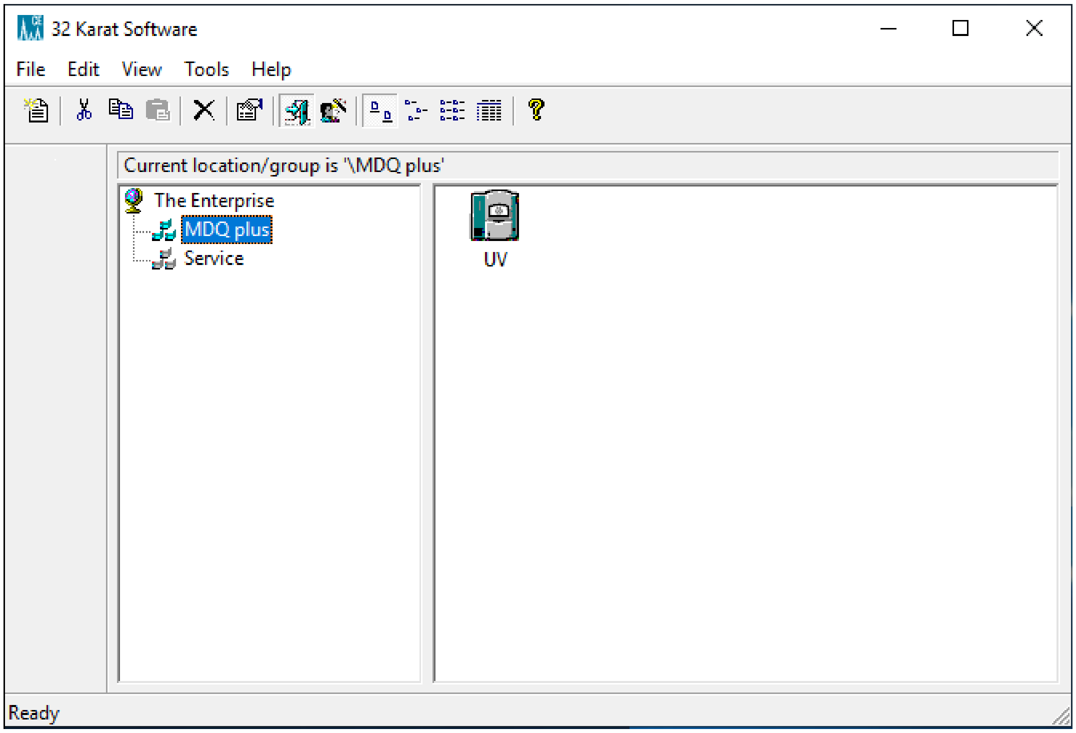
- Controlled access to functionality through customizable roles.
- Controlled access to project data on a role-by-role or group basis.
- Audit trails for instrument operation, maintenance, data acquisition, data review, and report generation.
- Electronic signatures that use a combination of user ID and password.

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. This document does not provide all of the information required for compliance with this or any other regulation. Using this or any other software product is not sufficient to assure compliance. The regulatory department of the organization can provide specific information about the policies and procedures that must be followed to be in compliance. Become familiar with the appropriate rules and regulations before configuring the security features of the 32 Karat software. The organization is ultimately responsible for regulatory compliance.

All system administration functions are accessed from the 32 Karat Software Enterprise window.

Tip! If the left pane is not visible in the Enterprise window, then click **View** > **Hierarchy Pane**.

Figure 1-1 32 Karat Software


32 Karat Software
File Edit View Tools Help
Current location/group is '\MDQ plus'
The Enterprise
MDQ plus
Service
UV
Ready

32 Karat Software System Administration Features

This section describes the system administration features in the 32 Karat software.

System Activity Log

The System Activity log is turned off by default and must be enabled by the system administrator. Refer to the section: Set General Options. This log includes all of the activity performed in the Enterprise window, such as system administration changes and instrument configurations.

Over time, the System Activity Log can become quite large. The software lets the user archive the log and remove the original file. Use the Log Viewer application to view the archived data. After a log is archived, the new System Activity Log indicates the date and location of the archive file. Refer to the section: View the System Activity Log.

Audit Trails

The Audit Trails track the history of data files and method files. The **Data file audit trail** is always active. **Method file audit trail** must be activated, but can be used in either administrator mode or standard mode.

Data File Audit Trail

A **Data file audit trail** trail records any process done to the data file after acquisition, such as when the data file is opened, analyzed, or signed off on with an electronic signature. These result sections might be different depending on the method used for the analysis. The **Data file audit trail** tracks these changes, as well as recording when the file was accessed, and by whom. A **Data file audit trail** stays 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 that the change occurred. Optionally, the user might be prompted to give a reason for the change. The **Method file audit trail** might be activated globally or for individual methods. After it is activated for a method, it cannot be turned off. If a method is saved with a new name, then a new **Method file audit trail** is created with the new method, and the old **Method file audit trail** stays with the original method.

Sequence Audit Trail

A **Sequence audit trail**, when active, records all of the changes made to a sequence file, along with the ID for the user who made the change, and the time that the change was made. Optionally, the user might be prompted to give a reason for the change. The **Sequence audit trail** might be activated globally or for individual methods. After it is activated for a sequence, it cannot be turned off. If a sequence is saved with a new name, then a new **Sequence audit trail** is created with the new sequence, and the old **Sequence audit trail** stays with the original sequence.

User Categories

The 32 Karat software recognizes three classes of users: system administrators, instrument administrators, and general users. There might be more than one user of each type, and any individual can serve in more than one role. The user is limited to the specific instruments and projects as specified by the administration policies set by the instrument and system administrator.

System Administrator

The system administrator can use all of the functions in the Enterprise screen of the software. If the system administrator does not have instrument administrator privileges, then they are not able to access the instrument configuration screen, which is opened by right-clicking on an instrument icon and then clicking **Configure**. The also can perform the following

The system administrator can use all functions in the software, as well as do the following:

- Enable logon

- Manage project settings
- Add or remove user access to the 32 Karat software
- Assign instrument or instrument administrator responsibility to users
- Manage project privileges for each user

If the system administrator has logged on, then anyone using the computer might have all privileges. The system administrator should always log out of administration mode before leaving the workstation. There can be more than one system administrator, and we recommend having a backup system administrator because there is no way to recover this account in the software.

Instrument Administrator

The instrument administrator can use the 32 Karat software to add, remove, rename, or configure instruments as well as to configure user access to instruments.

Users

Users are individuals who might be assigned some or all of the privileges listed in the following table. They are assigned to one or more projects and one or more instruments, and their privileges can vary both between projects and between instruments. Users have no administrative privileges.

Table 1-1 Privileges

Category	Selectable Privileges
Method	• **Open Method** • **Save Method** • **Properties** • **Instrument Setup** • **Integration Events** • **Peaks/Groups** • **Advanced** • **Custom Report** • **System Suitability** • **Review Calibration** • **Calibrate**

Table 1-1 Privileges (continued)

Category	Selectable Privileges
Data	• **Open Data** • **Save Data** • **Properties (Description)** • **Manual Integration Fixes**
Electronic Signature	• **Sign Data Files** • **Multiple Files Sign** • **Multiple File Revoke**
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[1]	• Not used.
Advanced Report	• **Open Advanced Report** • **Save Advanced Report**
Instrument Activity Log	• **Purge Log**

[1] The **Pre-treatment** privileges shown in the **Privileges** list are not used in the 32 Karat software and should be excluded.

Table 1-1 Privileges (continued)

Category	Selectable Privileges
Security	• **Access Common Folder**

Projects

In the 32 Karat software, projects organize computer files and access privileges to prevent unauthorized users from viewing or changing data and methods from projects to which they are not assigned. When a project is added, the system administrator specifies the access rights and location of the folder where all of the files used for acquiring data will be stored. For each user who has access to a project, specific privileges can be defined which will only apply in that project. A user might have different privileges in different projects.

Note: Project security will not be complete unless Windows security features are activated. This includes removing all **Delete** privileges for standard or non-administrative authenticated or local users. All other privileges should remain, such as **Read**, **Write**, **Execute**, and **Modify**. The **Modify** privilege should only be applied to project file folders after the laboratory has validated methods. Set the **Modify** privilege to prevent changes to the methods.

Only remove the **Modify** privilege from the project folders after the laboratory has validated the methods. Removing the **Modify** privilege prevents users from changing the names of the files for security purposes.

The Default Project

Users have full access to the predefined Default Project. The Default Project should not be used for any analyses for which compliance is important. For optimum security, remove access for all users and non-administrative authenticated users from this project in File Explorer and the 32 Karat software. Do not delete the Default Project because it also deletes the report templates. If the report templates are deleted then when a new project is added, the system administrator will have to manually add the report templates from a project other than the Default project.

Instruments

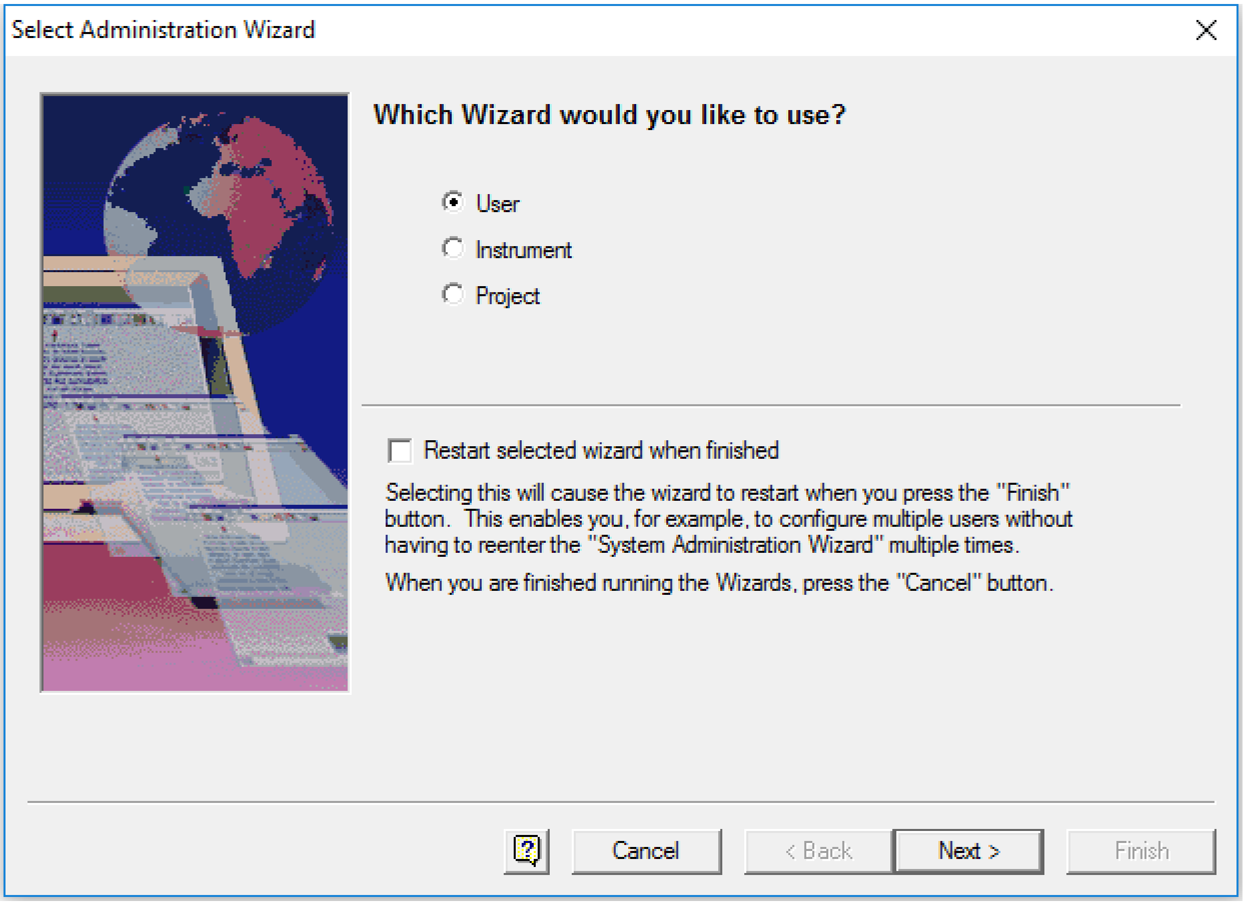
For the P/ACE MDQ Plus system, there is one instrument when the software is installed. The default configuration for the P/ACE MDQ Plus system only includes the UV detector.

Software Configuration 2

Use the Select Administration Wizard page to select a wizard to use to configure access and assign privileges. We recommend setting up the system administration in this order:

1. Activate system administration mode. Refer to the section: Activate the System Administration Mode.
2. Add users. Refer to the section: Add Users.
3. Add system administrators. Refer to the section: Add System Administrators.
4. Add projects. Refer to the section: Add Projects.
5. Add instruments. Refer to the section: Add an Instrument.

Figure 2-1 System Administration Wizards



Select Administration Wizard

Which Wizard would you like to use?

● User

○ Instrument

○ Project

□ Restart selected wizard when finished

Selecting this will cause the wizard to restart when you press the "Finish" button. This enables you, for example, to configure multiple users without having to reenter the "System Administration Wizard" multiple times.

When you are finished running the Wizards, press the "Cancel" button.

Wizard	Description
User	Use this wizard to assign system administration or instrument administration rights to users or groups defined on the system. Give users access to instruments and projects specified in the Enterprise window. For more information, refer to the section: Configure the 32 Karat Software .
Instrument	Use this wizard to assign user or group access to instruments and locations specified in the Enterprise window. For more information, refer to the section: Manage Instrument Access with the Instrument Wizard.
Project	Use this wizard to add new projects, assign users and groups to existing projects, change existing project definitions, or remove projects from the Enterprise window. A project consists of a set of Windows folders for the storage of methods, data, sequences, and templates, as well as a project description. Using projects makes sure that related data is stored in these designated directories that are consistent for all users. For more information, refer to the section: Manage Projects Using the Project Wizard.
Restart Selected Wizard When Finished	Select this check box to continue to use the selected wizard (User, Instrument, or Project) after the current wizard task has completed. For example, select this check box to set up multiple new projects without starting the Project Wizard again.

Activate the System Administration Mode

When the system administration mode is activated, several security and administrative features are enabled. When the 32 Karat software is installed, the system administration mode enables several system administrator features.

By default, one user is configured as a system administrator.

- User name: mdq, password: plus

When the 32 Karat software is installed, system administration mode is not enabled.

CAUTION: Potential Data Loss. Make sure that the user name and password for the system administrator is safely stored. If the user name, ID, or password for the system administrator is lost or forgotten, then the system administrator will not be able to access these features of the software or change them. After the system administrator mode is enabled, it can only be de-activated by the system administrator. Make sure to add additional backup system administrator accounts if required.

The security of the system is closely linked to the security of the Windows operating system. Make sure to match the security of the user or authenticated user in the operating system to the software user.

1. On the Windows desktop, double-click the 32 Karat icon.
   The Enterprise window opens.
2. Click **Tools** > **Options**.

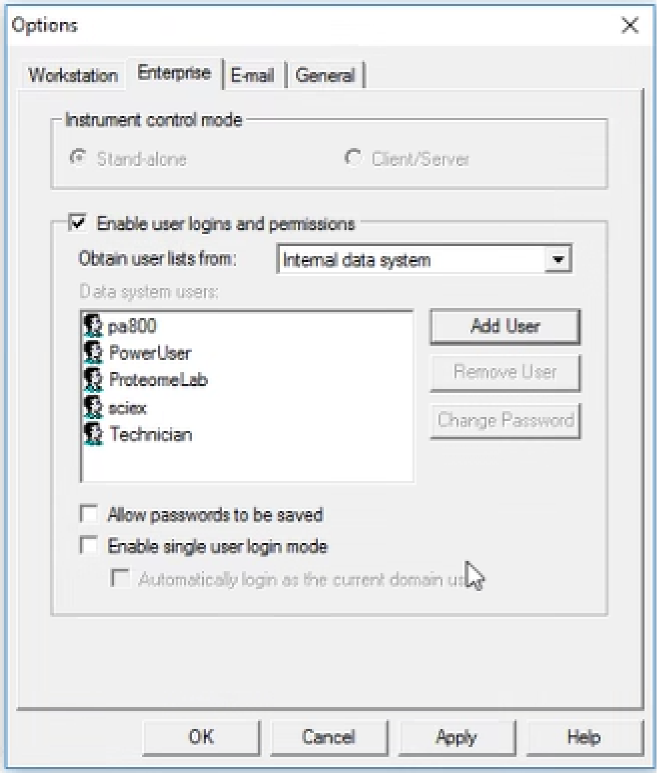
   By default, **System Administration Mode** is selected during a new installation.

   - If the Options dialog is not available, then system administration is already activated. A user must log on as a system or instrument administrator to access the Options dialog.
   - If the Options dialog is activated, then the Options dialog opens. Go to step 3 to enable system administration mode.
3. Open the Enterprise tab, click **Enable user logins and permissions**, and then click **OK**.
   The Options dialog closes.
4. As required, click **Tools** > **Enterprise Login** and then log on as a system administrator to configure the system administration features.

Add Users

1. From the 32 Karat software, on the Enterprise window, click **Tools** > **Options**. By default, **System Administration Mode** is selected during a new installation.
   The Options window opens.
2. From the **Obtain user lists from list**, select a location. Refer to the following tables to add and configure users.

Figure 2-2 Enterprise Tab in the Options Dialog: Internal data system



Instrument control mode

● Stand-alone ○ Client/Server

☑ Enable user logins and permissions

Obtain user lists from: Internal data system

Data system users:

- pa800
- PowerUser
- ProteomeLab
- sciex
- Technician

□ Allow passwords to be saved

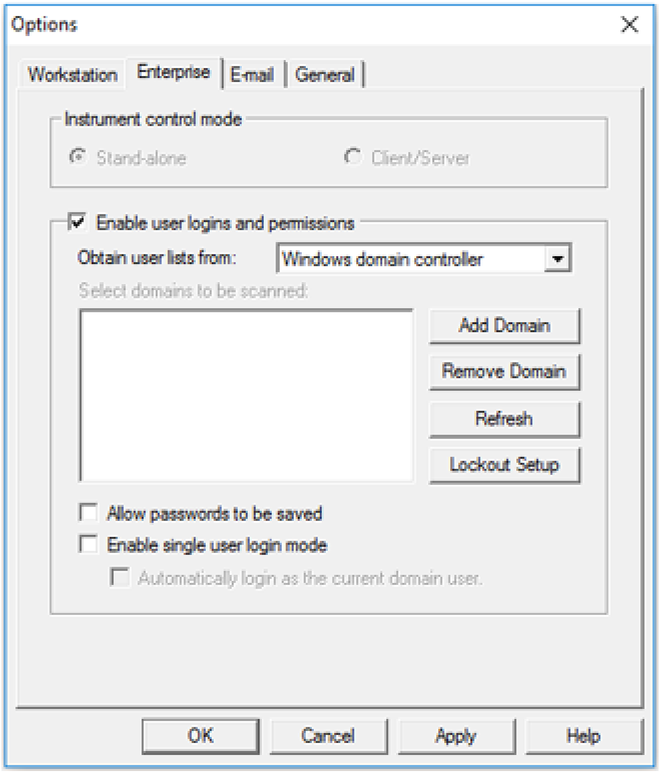
□ Enable single user login mode

□ Automatically login as the current domain us

Field	Description
Obtain user lists from	Select **Internal data system**: The list of users is maintained locally in the 32 Karat software. This option is preferred for small organizations with few users. The software administrator adds the user names and passwords. Users can be added or removed locally.
Add User	To add a user, click **Add User**, and then specify a user name and password. To assign privileges to users, refer to the section: Manage Access to the Software.
Remove User	**Note:** There is no option to cancel this action. The user is automatically removed. Select the user name from the list, and then click **Remove User**.
Change Password	To change the password for the selected user, click **Change Password**.

Field	Description
Allow passwords to be saved	Select to save the password of the user after initial logon. Subsequent logons will not require the user to enter a password unless the 32 Karat software is closed. This option is designed for systems where only one user will be using the workstation. **Note:** Be aware that allowing passwords to be saved decreases system security.
Enable single user login mode	Select to allow users to log on to all instruments once and not individually.
Automatically login as the current domain user (Domain Controller)	Select to enable the current Windows user to log on to the 32 Karat software for all instruments. This option applies only for the domain controller in use.

Figure 2-3 Enterprise Tab in the Options Dialog: Windows domain controller



Instrument control mode

● Stand-alone ○ Client/Server

☑ Enable user logins and permissions

Obtain user lists from: Windows domain controller

Select domains to be scanned:

□ Allow passwords to be saved

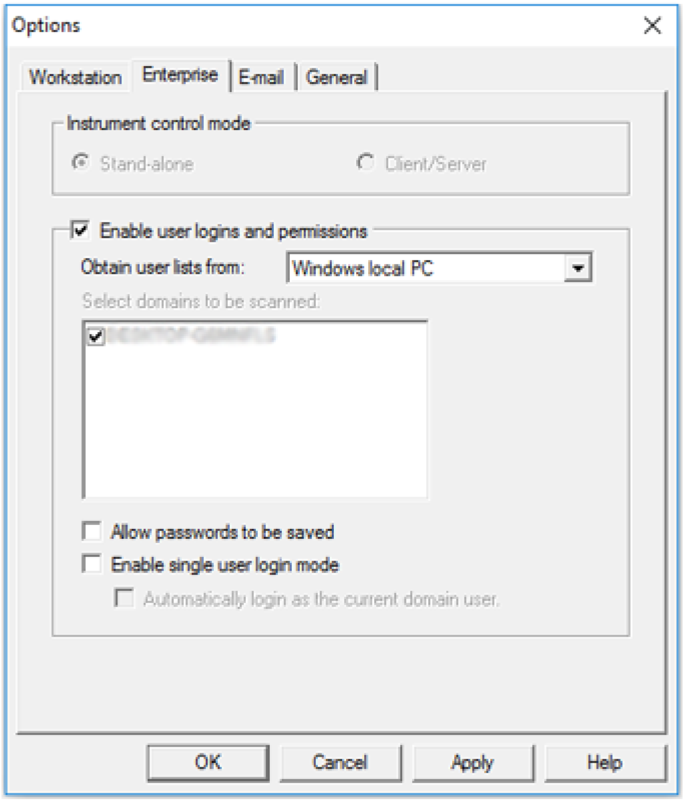
□ Enable single user login mode

□ Automatically login as the current domain user.

Field	Description
Obtain user lists from	Select **Windows domain controller**: The 32 Karat software workstation must be on a network. The list of potential users is 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, depending on how the network is configured. When the software is run under a domain controller, the user names and passwords are those already assigned to that domain. To add or remove users, a 32 Karat system administrator must also be a domain administrator. **Note:** If the Windows domain controller is used as the user list, and a domain on the network that is not under the control of the user is selected, then the user might lose access to the administrative features of the 32 Karat software, or the user might not be able to use the software at all. In this situation, individuals who have domain control must log in using their network password and assign administrative control of the 32 Karat software to the user. If control is lost, then contact sciex.com/request-support.
Select domains to be scanned (Domain Controller)	Select the domains to scan for users or groups. • Select **Add Domain** to specify a domain to be added to the possible domains listed. • Select **Remove** to remove a domain from the list. • Select **Refresh** to update the list of current domains.
Allow passwords to be saved	Select to save the password of the user after initial logon. Subsequent logons will not require the user to enter a password unless the 32 Karat software is closed. This option is designed for systems where only one user will be using the workstation. **Note:** Be aware that allowing passwords to be saved decreases system security.
Enable single user login mode	If selected, users can log on once to the entire system and will not need to log in to each instrument individually.

Field	Description
Automatically login as the current domain user (Domain Controller)	Select to enable the current Windows user to log on to the 32 Karat software for all instruments. This option applies only for the domain controller in use.

Figure 2-4 Enterprise Tab in the Options Dialog: Windows local PC



Options

Workstation | Enterprise | E-mail | General

Instrument control mode

● Stand-alone ○ Client/Server

☑ Enable user logins and permissions

Obtain user lists from: Windows local PC

Select domains to be scanned:

☑ [redacted]

□ Allow passwords to be saved

□ Enable single user login mode

□ Automatically login as the current domain user.

Field	Description
Obtain user lists from	Select **Windows local PC**: The 32 Karat software uses the local computer administrative tools for user lists and administrative accounts.

Field	Description
Allow passwords to be saved	Select to save the password of the user after initial logon. Subsequent logons will not require the user to enter a password unless the 32 Karat software is closed. This option is designed for systems where only one user will be using the workstation. **Note:** Be aware that allowing passwords to be saved decreases system security.
Enable single user login mode	Select to allow users to log on to all instruments once and not individually.
Automatically login as the current Windows user	Select to enable the current Windows user to log on to the 32 Karat software for all instruments. This option applies only to local Windows users.

3. Click **OK** to close the dialog.

Add System Administrators

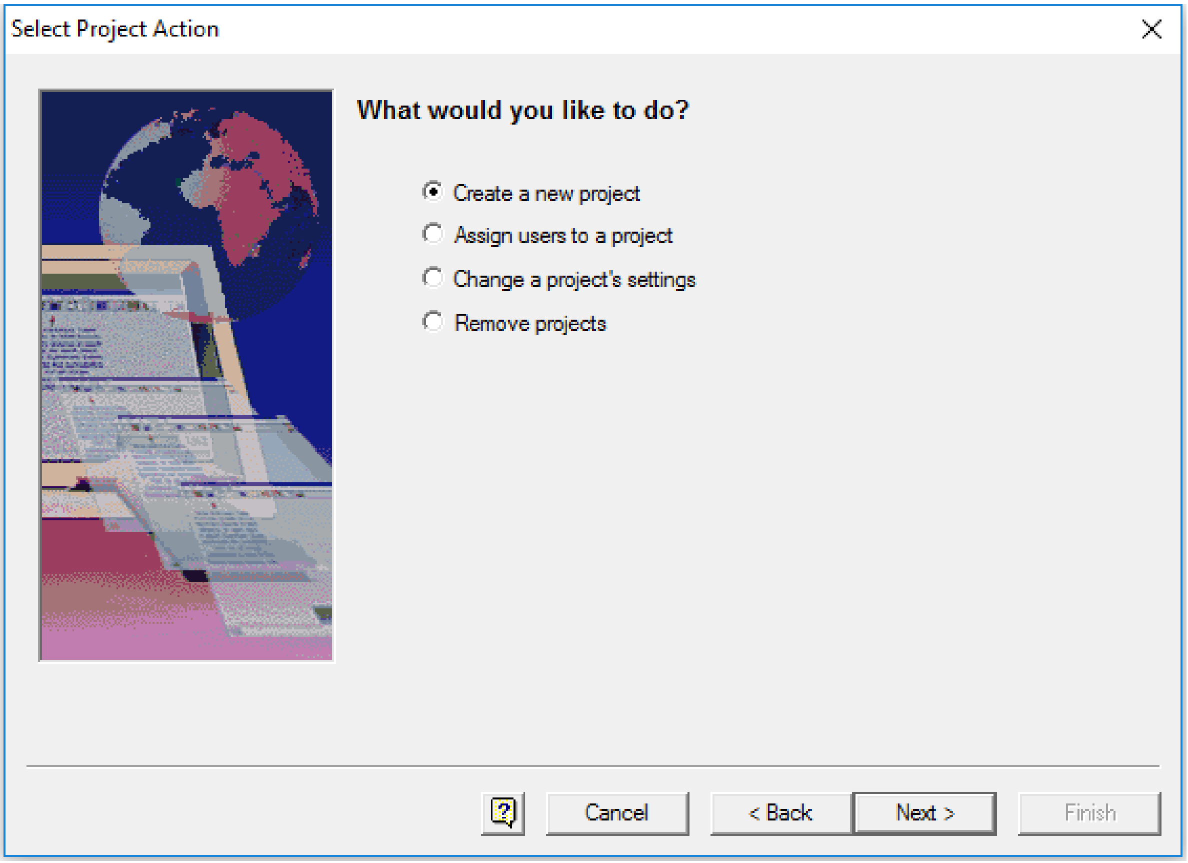
1. From the 32 Karat Software Enterprise window, click **Tools** > **System Administration Wizard**.
2. Click **User** and then click **Next** to continue.
   The Select User window opens.
3. Select the user to change and then click **Next**.
4. Do one of the following:
   - Select **System Administration** 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 check box is selected, then the user has no access to system administration functions or instrument administration functions.
5. After assigning privileges, click **Finish** to exit the User Wizard.

Add Projects

1. From the 32 Karat Software Enterprise window, click **Tools** > **System Administration Wizard**.
2. Click **Create a new project** to define a new project and then click **Next** to continue.

Figure 2-5 Select Project Action



Select Project Action

What would you like to do?

● Create a new project
○ Assign users to a project
○ Change a project's settings
○ Remove projects

The General Project Settings page opens.

3. Type a descriptive name and location for the project.

Tip! Click the folder icon to select the project location.

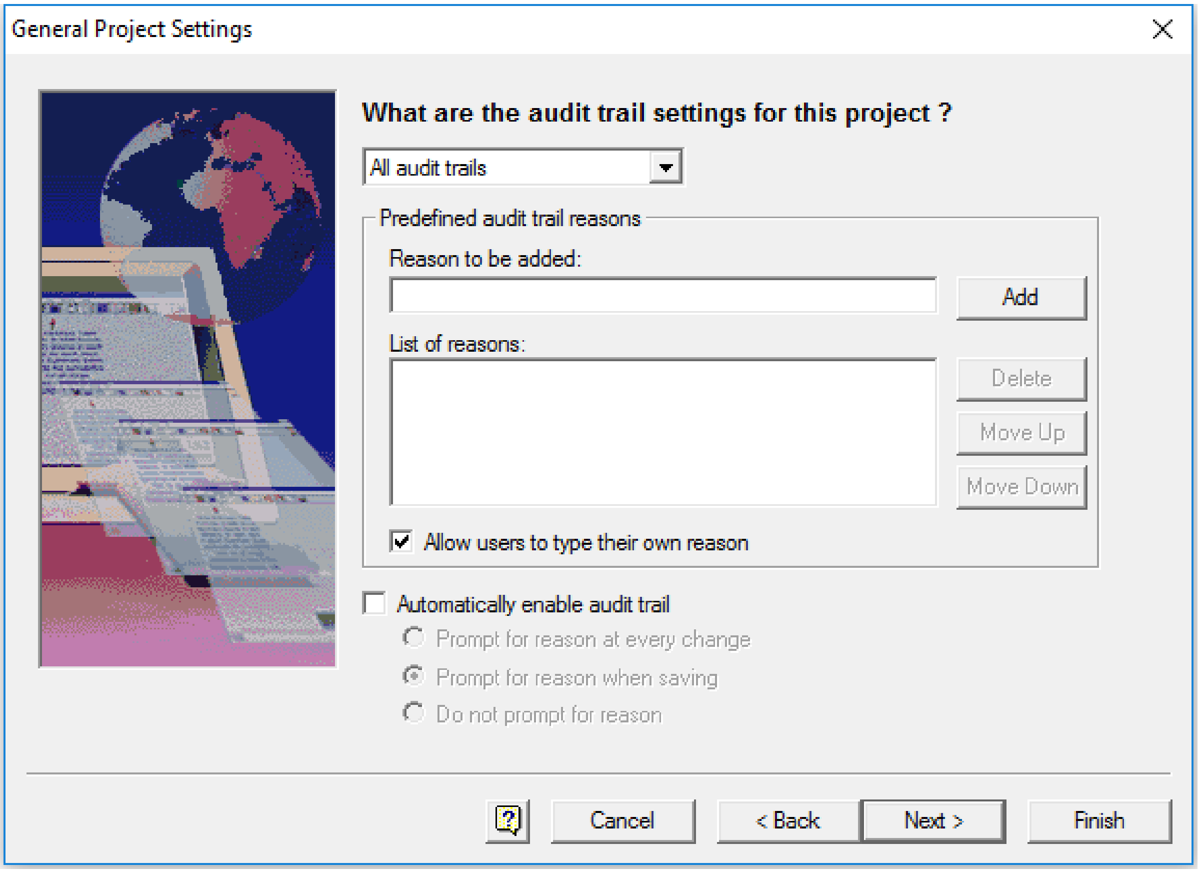
Note: If path names are manually typed, then all paths must be entered using universal naming conventions. For example, `\\ntserver\projects`.

The project folder is automatically populated with default folders: `Method`, `Data`, `Sequences`, and `Templates`.

4. After creating the projects, click **Next** to continue or click **Finish** to exit the Project Wizard.

5. On the General Project Settings page, from the list, select a specific audit trail for the project or click **All audit trails**.

Figure 2-6 General Project Settings Page



General Project Settings

What are the audit trail settings for this project ?

All audit trails

Predefined audit trail reasons

Reason to be added:

List of reasons:

☑ Allow users to type their own reason

□ Automatically enable audit trail

○ Prompt for reason at every change

● Prompt for reason when saving

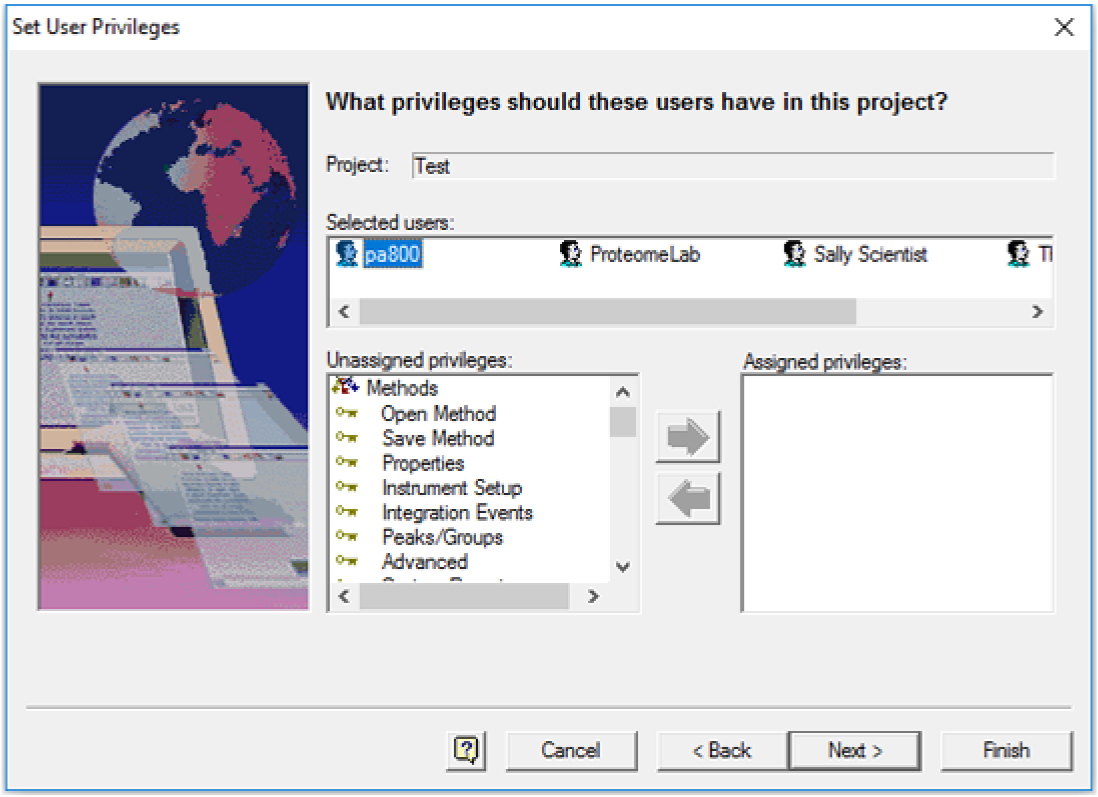
○ Do not prompt for reason

Field	Description
Predefined audit trail reasons	Shows the audit trail reasons that can be selected by users.
Reason to be added	To add a reason, type a reason and then click **Add**. The list of defined reasons is shown in the **List of reasons** field.
List of reasons	• To delete a reason, select the reason, and then click **Delete**. • To change the order of the reasons, select a reason, and then click **Move Up** or **Move Down**.
Allow users to type their own reason	Select to let users type their own audit trail reasons.

Field	Description
Automatically enable audit trail	Select to enable the audit trail for all files of the specified type added in this project. Select one of the following options: • **Prompt for reason at every change**. Select to prompt users for a reason whenever a change is made. • **Prompt for reason when saving**. Select to prompt users are for a reason for change only when a file is saved. • **Do not prompt for reason**. Select if a prompt for a reason will not be shown.

6. Click **Next** to continue or click **Finish** to exit the Project Wizard.
7. Select the electronic signatures applicable to the project.
8. Click **Next** to continue or click **Finish** to exit the Project Wizard.
   The Set User Privileges page is shown.

Figure 2-7 Set User Privileges



Set User Privileges

What privileges should these users have in this project?

Project: Test

Selected users: pa800, ProteomeLab, Sally Scientist, Tı

9. Select the user.

10. In the **Unassigned privileges** list, select the required privileges from those shown and then click the green arrow to move them to the **Assigned privileges** list. Privileges assigned from this location apply to the entire project. If required, individual user privileges can be changed later with the User Wizard.

    The privileges shown might be assigned as groups of items or as individual items.

    Note: The **Calibrate** privilege enables the user to run a calibration sample to update the method calibration. To add or change the calibration parameters in a method, the user must have the **Save Method** privilege assigned.

11. Click **Next** to continue or click **Finish** to exit the Project Wizard.
12. Select the level of signing authority for each user assigned to this project.

    A user can only revoke electronic signatures on a data file if no one with higher signing authority has signed the data file. If none of the users assigned to this project are assigned electronic signature roles for this project, then a message is shown.

    Note: Electronic signature roles apply only if domain user logons or local Windows PC user logons are used, not when the internal data system logon is used.

13. Click **Finish** to exit the Project Wizard.

Add an Instrument

1. Open the 32 Karat software.
2. In the Enterprise window, right-click, and then click **New** > **Instrument**.
3. Type a name for the instrument and then click anywhere in the window.
4. Add locations and instruments until the system enterprise matches the company or laboratory configuration.
5. Configure the instrument. Refer to the section: Manage Instrument Access with the Instrument Wizard.

Configure Electronic Signatures

Electronic signature features are set by the system administrator and allow the user to acquire, review, or sign off on data.

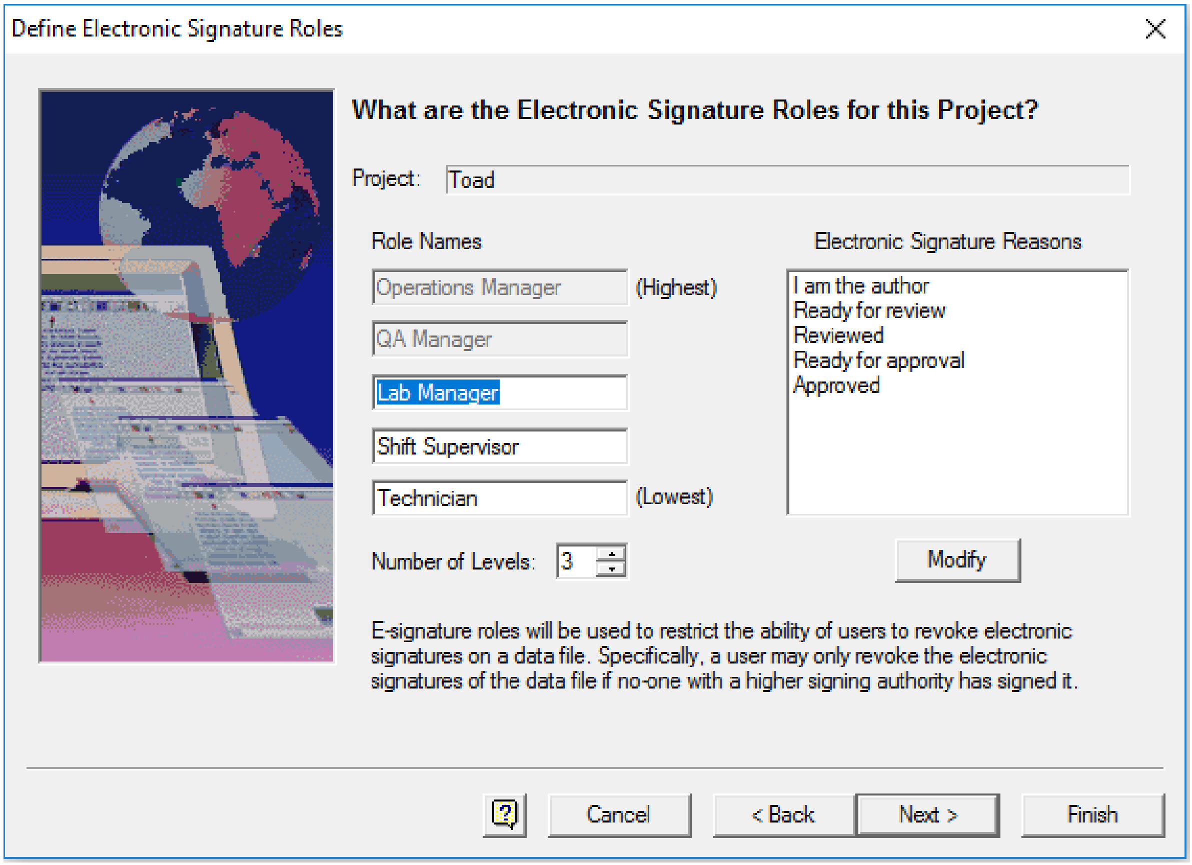
The 32 Karat software includes controls to facilitate 21 CFR part 11 compliance. Activating electronic signatures helps with this compliance process by enabling electronic audit trails to be generated in addition to electronic record keeping.

A user can only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file. If none of the users assigned to this project are assigned electronic signature roles for this project, a message is shown.

After someone has electronically signed a data file, it cannot be revoked by someone with a lower signature role. The electronic signature roles defined here specify the types of electronic signature roles for to this project.

1. From the **Tools** menu, click **System Administration Wizard**.
2. Click **Project** and then click **Next**.
3. Click **Change a project's settings** and then click **Next**.
4. Click the project and then click **Next**.
5. Click **Next**, change the audit trail settings, and then click **Next**.
6. Define the electronic signature roles for the selected project and then click **Finish** or **Next** to change any other settings for the project

Figure 2-8 Electronic Signature Roles Page



What are the Electronic Signature Roles for this Project?

Project: Toad

Role Names

Operations Manager (Highest)

QA Manager

Lab Manager

Shift Supervisor

Technician (Lowest)

Number of Levels: 3

Electronic Signature Reasons

I am the author
Ready for review
Reviewed
Ready for approval
Approved

E-signature roles will be used to restrict the ability of users to revoke electronic signatures on a data file. Specifically, a user may only revoke the electronic signatures of the data file if no-one with a higher signing authority has signed it.

Field	Description
Role Names	Shows the default names of the signature roles, along with the signature reasons. Change a role name by highlighting it, and then typing the new role name.
Number of Levels	Select the number of signature levels for this project. The default value is 3.
Electronic Signature Reasons	Current signature reasons are shown.

7. (Optional) To add, change, or delete Electronic Signature Reasons, click the **Modify** button.

   - To add a reason, type a reason and then click **Add**. The list of defined reasons is shown in the **List of reasons** field.
   - To delete a reason, select the reason, and then click **Delete**.
   - To change the order of the reasons, select a reason, and then click **Move Up** or **Move Down**.

   a. Click **OK** to save the new settings.
   The Define Electronic Signature Roles window opens.

8. Click **Finish** or **Next** to change any other settings for the project

Configure the 32 Karat Software

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

Use the software wizard to configure the following:

- Assign system administration rights to users or groups defined on the system.
- Assign instrument administration rights to users or groups defined on the system.
- Define the instruments or projects that are available to users or groups defined on the system.
- (Only applicable to non-domain workstations) Add or delete users from the system.

1. From the 32 Karat Software Enterprise window, click **Tools** > **System Administration Wizard**.
2. Click **User** and then click **Next** to continue.

Note: Select the **Restart selected wizard when finished** option to add or change more than one user. If this option is selected, then the User Wizard starts again after **Finish** is clicked.

The Select User window opens.

3. Select the user to change and then click **Next**.
4. After assigning privileges, click **Next** to continue or click **Finish** to exit the User Wizard.
5. In the Available Instruments list, select the instruments for this user by double-clicking the instrument.

Tip! Alternatively, select the instrument and then click the green arrow to move it to the Selected Instruments list.

Note: If no instruments are shown in the Available Instruments list, then expand the **Enterprise** icon by double-clicking locations until the required instruments are shown.

Assign all instruments in a laboratory or location to a user or group by selecting the entire location from the Available Instruments list. If a location (for example, Enterprise) is shown in the Selected Instruments list, then all instruments in that location are selected.

6. After selecting the instruments, click **Next** to continue or click **Finish** to exit the User Wizard.
7. In the Available Projects list, select the projects for this user by double-clicking them.

Tip! Alternatively, select the project and then click the green arrow to move it to the Selected Projects list.

8. After selecting projects, click **Next** to continue or click **Finish** to exit the User Wizard
9. Select the required privileges from those shown in the Unassigned privileges list and then click the green arrow to move them to the Assigned privileges list. The privileges shown might be assigned as groups of items or as individual items.

Note: The **Calibrate** privilege lets the user run a calibration sample to update the method calibration. To add or change 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.

10. After setting user privileges for each project, click **Next** to continue or click **Finish** to exit the User Wizard.

11. Select the level of signing authority for the user. A user can only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file.

    Note: Electronic signature roles apply only if domain user logons or local Windows PC user logons are used, not when the internal data system logon is used.

12. After the electronic signature roles for the user are defined, click **Finish** to exit the User Wizard.

Instrument Logon

After users have been added to the data system and their privileges assigned to various instruments and projects in the database, they can start instruments to which they have been assigned.

If users attempt to open an instrument from the 32 Karat Software Enterprise window, then they are prompted to enter their user name, their password, and select the project to which they are logging on.

If the Windows domain logon or domain controller option has been selected, then the domain selection window is also shown, which the user can select as well.

All instrument logons are saved to the instrument activity log, and the system administrator can also set up additional security features to prevent unauthorized access to the system. Refer to the section: Worksheets.

Manage Access to the Software 3

Use the System Administration Wizards to easily manage the system administration functions in the 32 Karat software. System administrators can add projects, add users, and assign the user permissions. Projects are represented by Windows folders that are recognized by the software.

Access for each project is set by the system administrator.

Note: The project and instrument name must match what is shown in the 32 Karat software. Do not use the special character “-” in a project or instrument name.

Three wizards are available. Each provides a pre-defined, step-by-step process for managing users and projects.

Manage Projects Using the 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 32 Karat Software Enterprise window. A project consists of Windows folders used to create folders to store methods, data, sequences, and templates, along with a project description.

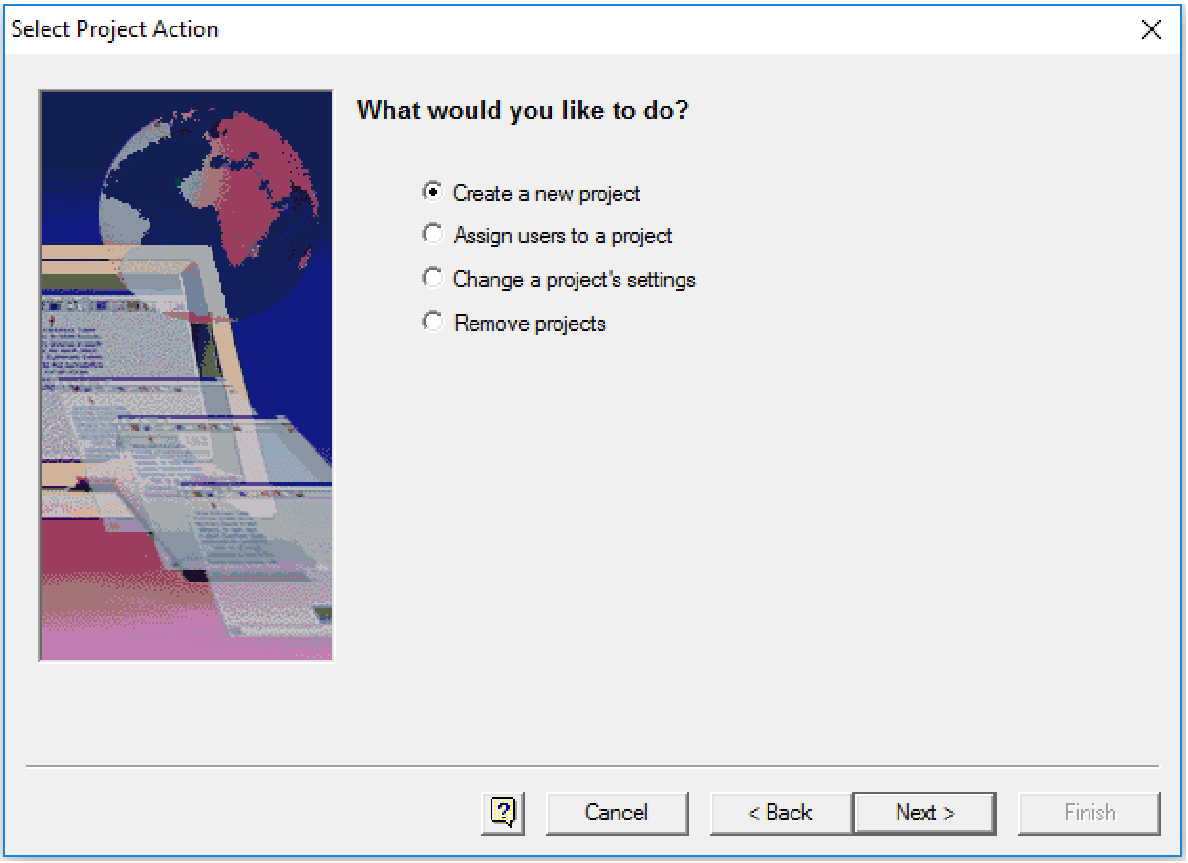
Projects facilitate data management by making sure that related data are stored in designated folders that are consistent for all users.

1. From the 32 Karat Software Enterprise window, click **Tools** > **System Administration Wizard**.
2. Click **Project** and then click **Next** to proceed.

   Note: Select the **Restart selected wizard when finished** option to add or edit more than one project. When this option is selected, the Project Wizard starts again after **Finish** is clicked.

   The Select Project Action dialog opens.
3. Select one of the following options:

Figure 3-1 Select Project Action Dialog



Select Project Action

What would you like to do?

● Create a new project
○ Assign users to a project
○ Change a project's settings
○ Remove projects

4. After assigning projects, click **Next** to continue. Refer to the sections: Add Projects, Assign Users to a Project, and Remove Projects.

Assign Users to a Project

1. From the 32 Karat software Enterprise window, click **Tools** > **System Administration Wizard**.
2. Click **Project** and then click **Next** to proceed.
3. Click **Assign users to a project** and then click **Next**.
   The Select Project window is shown.
4. Select the project to which to assign users and click **Next**.
5. Select the number of signature levels for this project. The default level is `3`.

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

   The current signature reasons are shown.

6. To add, change, or delete **Electronic Signature Reasons**, click **Modify**.
   - To add a reason, type a reason and then click **Add**. The list of defined reasons is shown in the **List of reasons** field.
   - To delete a reason, select the reason, and then click **Delete**.
   - To change the order of the reasons, select a reason, and then click **Move Up** or **Move Down**.
7. Click **OK** to save the new settings.
   The Define Electronic Signature Roles window opens.
8. Click **Next** to continue to the Select Users window or click **Finish** to exit the Project Wizard.
9. Select the user.
10. In the **Unassigned privileges** list, select the required privileges from those shown and then click the green arrow to move them to the **Assigned privileges** list. Privileges assigned from this location apply to the entire project being added. Individual user privileges might then be later modified using the User Wizard interface.

    The privileges shown might be assigned as groups of items or as individual items.

    Note: The Calibrate privilege enables the user to run a calibration sample to update the method calibration. To add or change the calibration parameters in a method, the user must have the Save Method privilege assigned.
11. Click **Next** to continue to the Select Users window or click **Finish** to exit the Project Wizard.
12. Select the level of signing authority for each user assigned to this project.

    A user can only revoke electronic signatures on a data file if no one of higher signing authority has signed the data file. If none of the users assigned to this project are assigned electronic signature roles for this project, a message is shown.

    Note: Electronic signature roles apply only if domain user logons or local Windows PC user logons are used, not when the internal data system logon is used.
13. Click **Finish** to exit the Project Wizard.

Manage Instrument Access with the Instrument Wizard

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

1. From the 32 Karat Software Enterprise window, click **Tools** > **System Administration Wizard**.
2. Click **Instrument** and then select **Next** to continue.

Note: Select the **Restart selected wizard when finished** check box to add or edit more than one instrument or location. When this option is selected, the Instrument Wizard starts again after **Finish** is clicked.

3. Select the individual instrument or the location containing multiple instruments to which to assign a user or group access and then click **Next**.

   The Select Users window opens.

4. Do one of the following to select users:

Table 3-1 Select Users

Field	Description
Internal Data System	Select to highlight the name of the user to add or change. Then select one of the green or red arrows to move the user to or from the instrument.
Windows Domain Controller	Select the domain from the list of domains available. A domain is a functional portion of the network that has been set up by the Windows domain controller. After selecting the domain, specify the user or group and then click **Check names** to locate them in the domain. • To select a group, click **Groups** and then specify the group name and select **Check names** to locate the group on the domain. Then select the valid group and click the green arrow to move the group to the instrument. • To select an individual user, select **Users** to specify a user name and locate the users in the domain. Then click the green arrow to move the user to the instrument.
Windows Local PC	Managed by Windows Local PC administrative tools.

5. Click **Finish** to exit the Instrument Wizard.

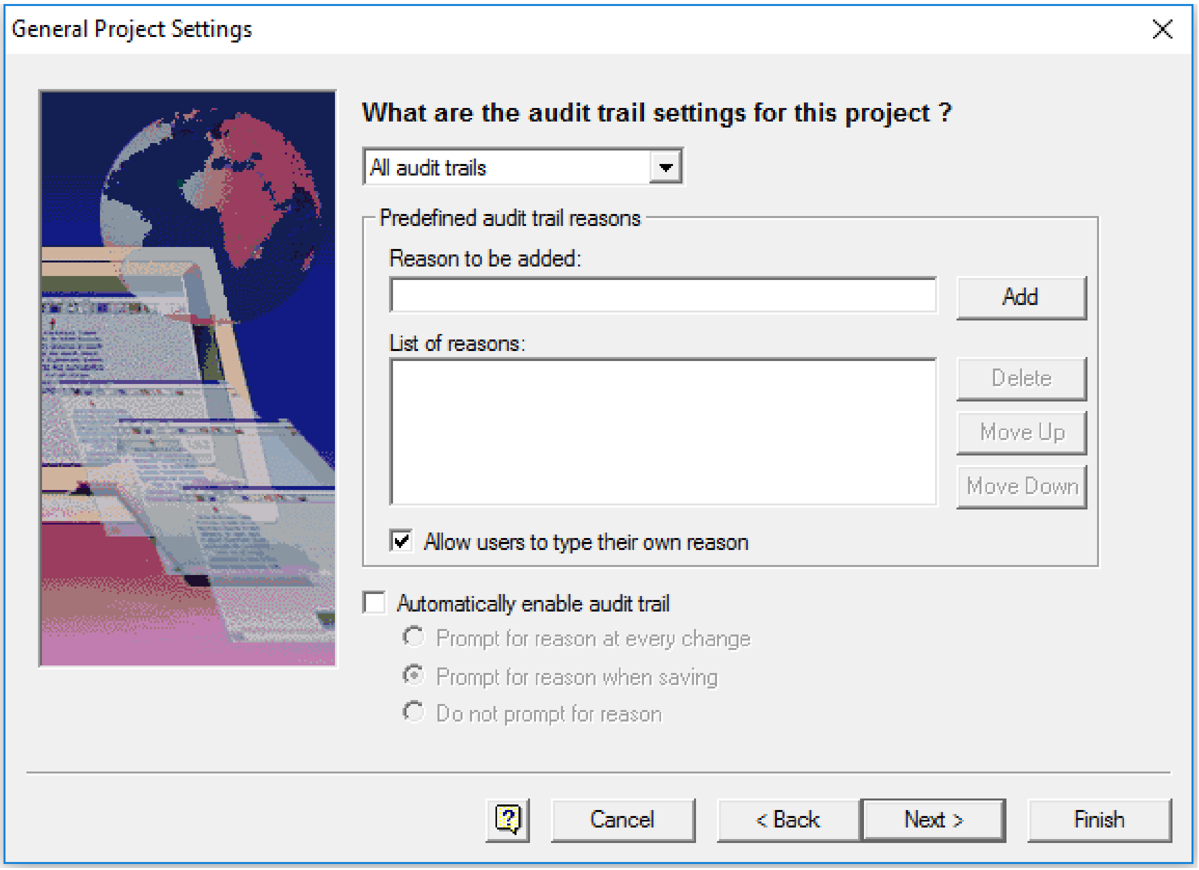
Change Project Settings

1. In the System Administration Wizard, select **Project**.
2. Click **Change a project's settings** and then click **Next**.
   The General Project Settings window is shown.
3. Select the project to which to assign users and then click **Next**.

   When changing project settings, the project name or file locations cannot be changed. This window lets users specify or change the optional text description, for the selected project.
4. Click **Next** to continue or click **Finish** to exit the Project Wizard.

5. Select a specific audit trail to which the settings will apply or click **All audit trails**.

Figure 3-2 General Project Settings



General Project Settings

What are the audit trail settings for this project ?

All audit trails

Predefined audit trail reasons

Reason to be added:

List of reasons:

☑ Allow users to type their own reason

☐ Automatically enable audit trail

○ Prompt for reason at every change

● Prompt for reason when saving

○ Do not prompt for reason

Field	Description
Predefined audit trail reasons	Define the audit trail reasons that can be selected by users.
Reason to be added	• To add a reason, type a reason and then click **Add**. The list of defined reasons is shown in the **List of reasons** field. • To delete a reason, select the reason, and then click **Delete**. • To change the order of the reasons, select a reason, and then click **Move Up** or **Move Down**.
Allow users to type their own reason	If selected, allows users to type a reason.

Field	Description
Automatically enable audit trail	If selected, the audit trail is automatically enabled for all files of the specified type added in this project.
Prompt for reason at every change	If selected, users are prompted for a reason whenever a change is made.
Prompt for reason when saving	If selected, users are prompted for a reason for change only when a file is saved.
Do not prompt for reason	If selected, a prompt for reason is never shown.

6. Click **Next** to continue or click **Finish** to exit the Project Wizard.
7. Select the electronic signatures applicable to the project.

Table 3-2 Electronic Signature

Field	Description
Role Names	Default names for the various signature roles are shown, along with the signature reasons. Change a role name by highlighting it, and then changing the role name.
Number of Levels	Select the number of signature levels for this project. The default is 3. After someone has electronically signed a data file, it might not be revoked by someone with a lower signature role.
Electronic Signature Reasons	Current signature reasons are shown. To add, change, or delete Electronic Signature Reasons, click the **Modify** button. • To add a reason, type a reason and then click **Add**. The list of defined reasons is shown in the **List of reasons** field. • To delete a reason, select the reason, and then click **Delete**. • To change the order of the reasons, select a reason, and then click **Move Up** or **Move Down**.

8. Click **Next** to continue or click **Finish** to exit the Project Wizard.
9. Select the user.
10. In the **Unassigned privileges** list, select the required privileges from those shown and then click the green arrow to move them to the **Assigned privileges** list. Privileges assigned

from this location apply to the entire project being added. Individual user privileges might then be changed later with the User Wizard interface.

The privileges shown can be assigned as groups of items or as individual items.

Note: The **Calibrate** privilege enables the user to run a calibration sample to update the method calibration. To add or change the calibration parameters in a method, the user must have the **Save Method** privilege assigned.

11. Click **Next** to continue or click **Finish** to exit the Project Wizard.
12. Select the level of signing authority for each user assigned to this project.

    A user can only revoke electronic signatures on a data file if no one with higher signing authority has signed the data file. If none of the users assigned to this project are assigned electronic signature roles for this project, then a message is shown.

    Note: Electronic signature roles apply only if domain user logons or local Windows PC user logons are used, not when the internal data system logons are used.

13. Click **Finish** to exit the Project Wizard.

Remove Projects

1. In the System Administration Wizard, select **Project**.
2. Click **Remove projects** and then click **Next**.
   The Select Project window is shown.
3. Select the project to remove and then click **Finish**.
   The selected project is removed from the system.

Note: When a project is removed using the wizard, access to its directories is removed. The actual data directories defined for the project are not deleted.

Additional Features 4

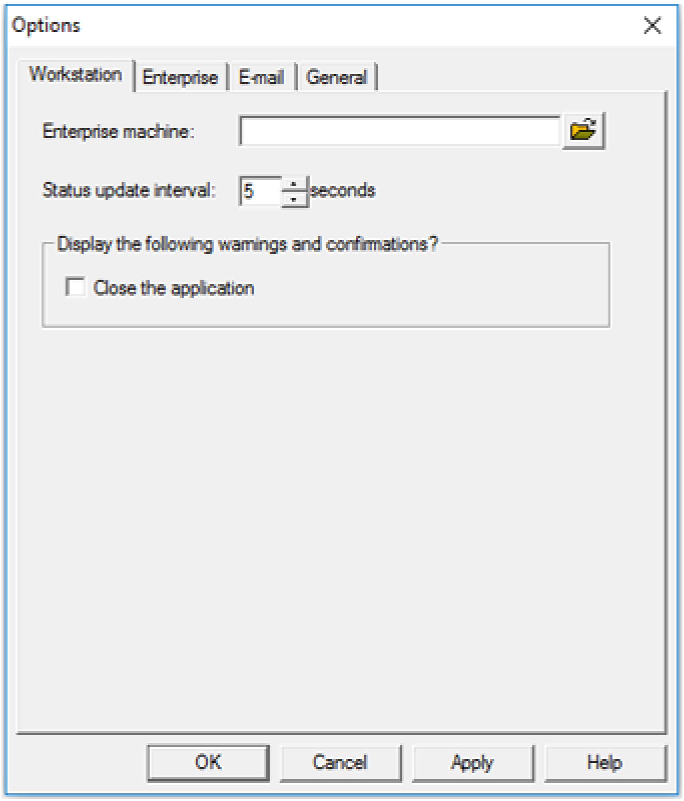
The System Administrator can add reports for various user aspects of the P/ACE MDQ Plus system, assign global security settings to the system, and add a system activity log.

The Options Dialog

The Options dialog is where system administration mode is enabled or disabled, users and passwords are added, and email notifications configured. In addition, system administrators can configure logging, audit trails, activity logs, extended security, and software behavior when the computer is idle.

Workstation Tab

Figure 4-1 Workstation Tab Options



Enterprise machine:

Status update interval: 5 seconds

Display the following warnings and confirmations?

☐ Close the application

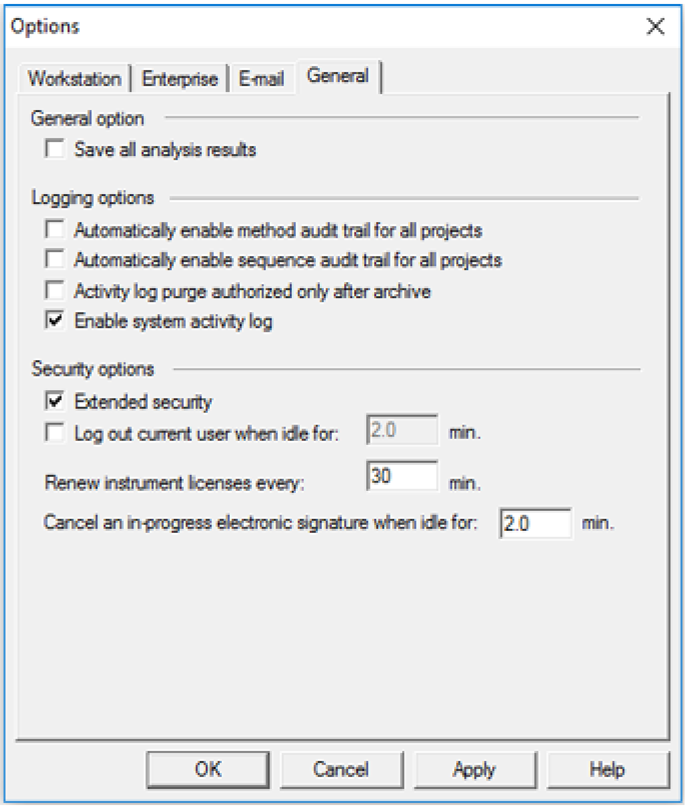
Field	Description
Enterprise machine	Leave this field blank.
Status update interval	From the 32 Karat Software Enterprise window, click **View** > **Detail** to show the Instrument status. The current status of each instrument is shown. For example, **Idle**, **Available**, **In Use**.
Display the following warnings and confirmations	Select this option to open a confirmation dialog when the 32 Karat software is closed.

Set General Options

1. On the Windows desktop, double-click the 32 Karat icon.
   The Enterprise window opens.
2. Click **Tools** > **Options** > **General**. This option allows the system administrator to automatically assign security settings to the entire system.

   Note: We recommend that **Enable system activity log** is selected. Refer to the following figure.

Figure 4-2 General Tab



General option

☐ Save all analysis results

Logging options

☐ Automatically enable method audit trail for all projects

☐ Automatically enable sequence audit trail for all projects

☐ Activity log purge authorized only after archive

☑ Enable system activity log

Security options

☑ Extended security

☐ Log out current user when idle for: 2.0 min.

Renew instrument licenses every: 30 min.

Cancel an in-progress electronic signature when idle for: 2.0 min.

Field	Description
Save All Analysis Results	If this check box is selected, then each time a data file is analyzed, the results are saved in the data file and are identified with the user name and date of the analysis. Identification makes it possible to open a specific result from the Open Data dialog in the Instrument Control program window, using the **Open with Results** option using the Options section and then selecting **From Results for Method** and the **Results date and time** in the **Results** field using the ellipses button. If this check box is not selected, then only the original and most recent results are saved in the file.
Logging Options	
Automatically enable method audit trail	If this option is selected, then the method audit trail is enabled whenever a method is saved.

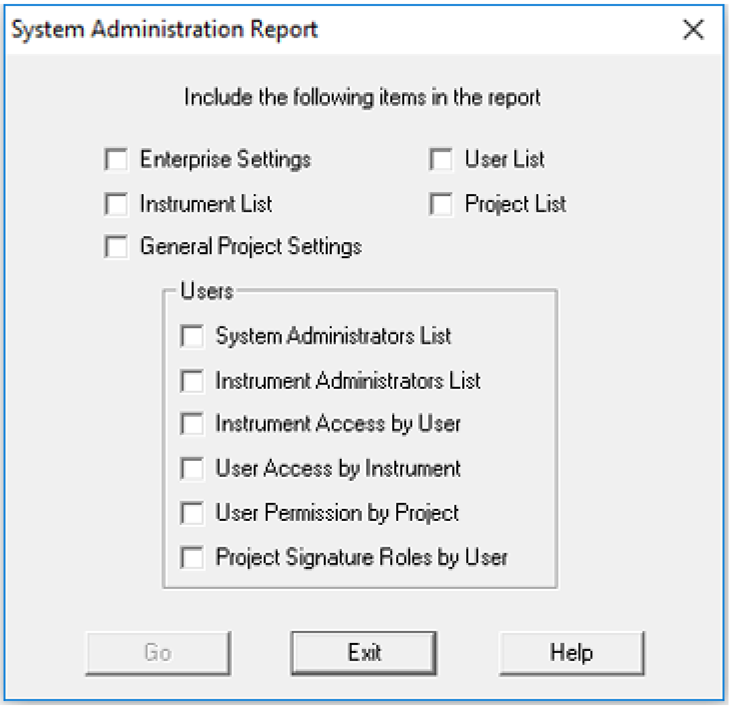
Field	Description
Automatically enable sequence audit trail	If this option is selected, then the sequence audit trail is enabled whenever a sequence is saved.
Activity log purge authorized only after archive	If this option is selected, then the instrument activity log must be archived before it can be purged.
Enable system activity log	If this option is selected, then the system activity log is enabled. After the log is enabled, it cannot be turned off. We recommended that this feature is enabled.
Security Options	
Extended Security	If this option is selected, then a checksum is calculated whenever a data file is closed. When the file is subsequently opened, its checksum is verified first. If the verification fails, then 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 have read/execute rights to project directories for which they have rights. • All non-system administrators 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 add 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 added in project subfolders, but only through the 32 Karat software.

Field	Description
Log out Current User When Idle For	If this option is selected, then type a number, in minutes. If no mouse or keyboard activity is detected during the specified number of minutes in system administration mode, then the system does the following: • Cancel any open dialogs • Cancel any wizard in progress • Log out of Administrative Mode **Note:** This feature applies to the Enterprise window only, and does not affect any open instrument program windows.
Cancel an In-Progress Electronic Signature When Idle For	If an electronic signature is in progress, then it will be cancelled if there is no input for the specified number of minutes.

System Administration Report Utility

The 32 Karat software includes a system administration report utility. Use this utility to show the configuration for project settings, users and permissions, instrument configurations, and enterprise-wide settings. Refer to the following figure.

Figure 4-3 System Administration Report Utility



System Administration Report

Include the following items in the report

□ Enterprise Settings

□ Instrument List

□ General Project Settings

□ User List

□ Project List

Users

□ System Administrators List

□ Instrument Administrators List

□ Instrument Access by User

□ User Access by Instrument

□ User Permission by Project

□ Project Signature Roles by User

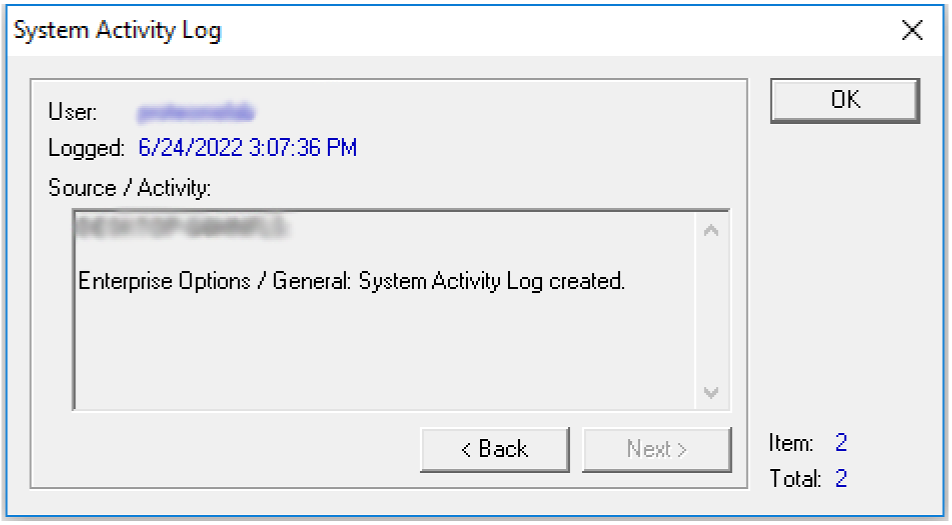
Create System Administration Report

1. From the **Tools** menu, click **System Administration Report**.
2. elect the options and then click **Go**.
   The Report window opens
3. (Optional) Click **File** > **Print Report** in the report to print the report.
4. Click the **Close** box to close the report.

View the System Activity Log

1. From the 32 Karat software Enterprise window, click **Tools** > **Enterprise Login** and then log on as an instrument or system administrator.
2. Click **File** > **System Activity Log** > **Display Log**.

Figure 4-4 System Activity Log



System Activity Log

User: [redacted]

Logged: 6/24/2022 3:07:36 PM

Source / Activity:

[redacted]

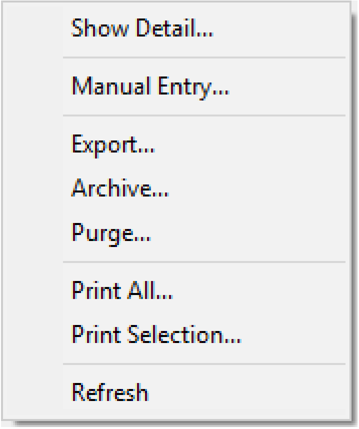
Enterprise Options / General: System Activity Log created.

Item: 2

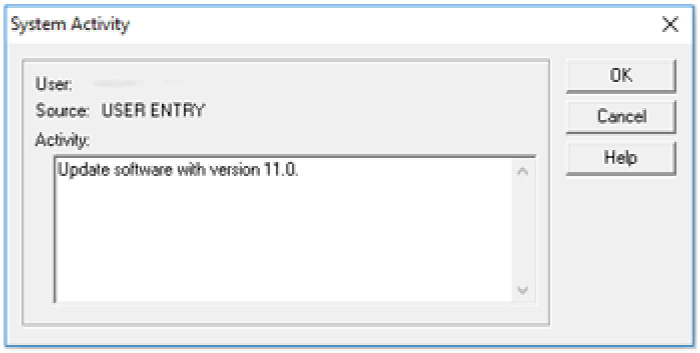
Total: 2

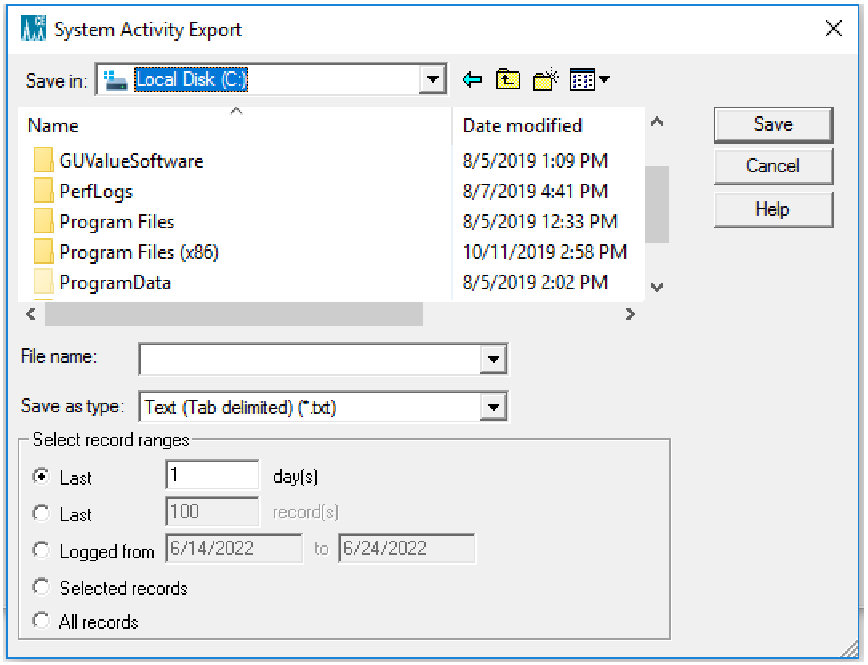
3. Right-click in the **System Activity Log** for additional actions.

Figure 4-5 System Activity Log Menu Options



Menu Item	Description
Show Detail	Click to show the information for the currently selected entry.

Menu Item	Description
Manual Entry	a. Click to add a manual entry to the log. b. Type the information and then click **OK**. **Figure 4-6 System Activity Manual Entry Dialog**  User: Source: USER ENTRY Activity: Update software with version 11.0.

Menu Item	Description
Export	Only available to system administrators. **Figure 4-7 System Activity Export**  System Activity Export Save in: Local Disk (C:) Name — Date modified GUValueSoftware — 8/5/2019 1:09 PM PerfLogs — 8/7/2019 4:41 PM Program Files — 8/5/2019 12:33 PM Program Files (x86) — 10/11/2019 2:58 PM ProgramData — 8/5/2019 2:02 PM File name: Save as type: Text (Tab delimited) (*.txt) Select record ranges ● Last 1 day(s) ○ Last 100 record(s) ○ Logged from 6/14/2022 to 6/24/2022 ○ Selected records ○ All records a. Click to export the log or the selected range of the log to a specific file. b. Type a file name in the **File name** field. c. Select a file type from the **Save as type** list. d. Select a record range. e. Click **Save** to save the system activity log for the range selected in the file specified.
Archive	Only available to system administrators. In the dialog that opens, 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 opened from: `C:\32Karat\LogViewer.exe`. **Tip!** Access the archive from the Start menu: Click **Start** > **P/ACE MDQ Plus Software** > **Log Viewer**.

Menu Item	Description
Purge	Only available to system administrators. The purge activity varies based on options selected in the Options dialog. Refer to the section: Set General Options. • If the **Activity Log Purge authorized only after archive** option is selected, then the System Activity Log Archive dialog opens first. After confirmation, the log is purged. • If the **Activity Log Purge authorized only after archive** check box is not selected, then a confirmation message is shown. If the user confirms, then the purge operation occurs. After the log is purged, an entry is added to the System Activity Log stating that the purge occurred.
Print all	Click to print all of the rows in the log.
Print Selection	Click to print only the selected rows of the log.
Refresh	Click to update the log.

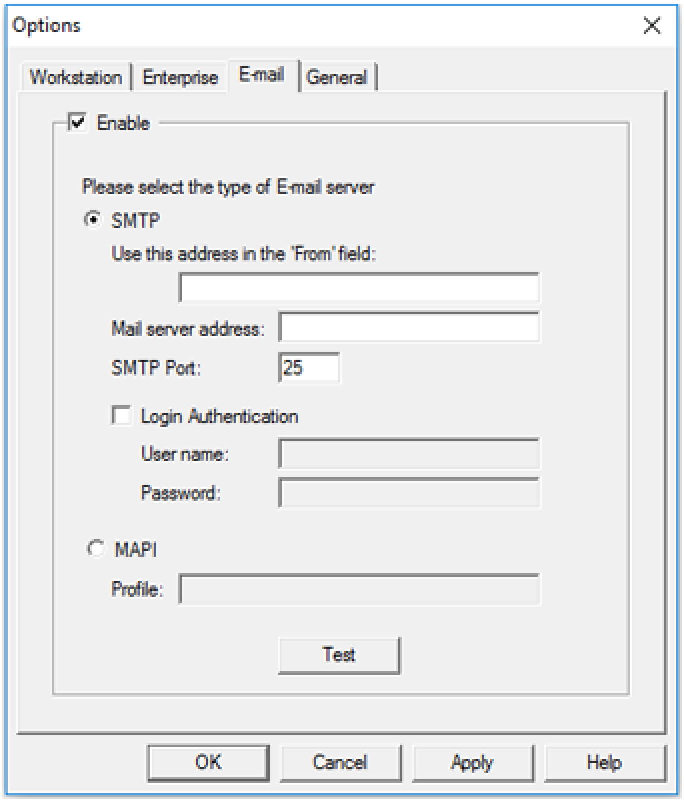
4. Click **Close** to close the **System Activity Log** dialog.

Configure Email Notifications

For more information about configuring events and generating email notifications, refer to the document: *Help* that comes with the software.

1. On the Windows desktop, double-click the 32 Karat icon.
   The Enterprise window opens.
2. Click **Tools** > **Options** > **General**. This option allows the system administrator to automatically assign security settings to the entire system.
3. Click the E-mail tab and then refer to the following table to configure notifications.

Figure 4-8 Email Tab Options



Options

☑ Enable

Please select the type of E-mail server

● SMTP

Use this address in the 'From' field:

Mail server address:

SMTP Port: 25

□ Login Authentication

User name:

Password:

○ MAPI

Profile:

Field	Description
Enable	Select this check box to enable the settings for email. When cleared, 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	Specify an email address of a valid user.
Mail server address	Specify the SMTP-compliant email address of the local mail server to which 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 might 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.

Field	Description
Profile	Specify the MAPI Profile to be used for sending email.
Test	Select this option to have the system try to • connect to the email server and test the port (for SMTP) • determine if the profile exists on the server (for MAPI) This function shows a message indicating the success or failure of the connection attempt.

Example Administration Setup 5

In this section, a hypothetical laboratory is described. To suit the needs of this laboratory, various system administration features are enabled. To help organize the system, use the worksheets in the section: Worksheets

Laboratory Personnel

In this example, a small pharmaceutical laboratory has three 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 system 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 described in the following sections.

Table 5-1 Laboratory Personnel

Personnel	Description
Data System Users	The following users are added to the data system: • LabMgr: System Administrator • InstAd: Instrument Administrator • Tech: Standard User Refer to the section: Assign Users to a Project.

Table 5-1 Laboratory Personnel (continued)

Personnel	Description
System Projects	The lab manager adds the following projects: • Protein • Nucleic Acid • Small Molecules • Performance Refer to the section: Add Projects.
Project Access	The lab manager grants project access as follows: • LabMgr: Protein, Nucleic Acid, Small Molecules, Performance • InstAd: Performance • Tech: Protein Refer to the section: Assign Users to a Project.
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 Refer to the section: Configure Electronic Signatures.
System Instruments	The Instrument Administrator adds the following instruments: • Protein: LabMgr, InstAd, and Tech as users • Development: LabMgr and InstAd as user • Performance: InstAd as user Refer to the "P/ACE MDQ Plus Instrument Configuration” topic in the Configuration section of the 32 Karat software *Help*.

Table 5-1 Laboratory Personnel (continued)

Personnel	Description
Users	The lab manager hires a bio-statistician. Among other responsibilities, this employee reviews data acquired by the technician before submission to the manager for approval. The system administrator changes the Protein Project as follows: 1. The lab manager selects the Enterprise login from the **Tools** menu and then enters the appropriate user name and password. 2. The lab manager selects **Options** from the **Tools** menu. The Analyst User is added to the Enterprise tab. 3. The lab manager opens the System Administration Wizard from the **Tools** menu. 4. The lab manager uses the Project Wizard to change 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.
Electronic Signature Roles	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

After the changes are complete, the Lab Manager clicks **Enterprise Logout**. This example shows how the system administration can be used in a laboratory setting.

Use copies of the worksheets to help plan the System Administration settings that are most appropriate for the laboratory. Refer to the section: Worksheets

Worksheets 6

Table 6-1 Enterprise Options Dialog

Project Name	**User**
Methods	
Open Method	
Save Method	
Properties	
Instrument Setup	
Integration Events	
Peaks/Groups	
Advanced	
Custom Report	
System Suitability	
Review Calibration	
Calibrate	
Data	
Open Data	
Save Data	
Properties (Description)	
Manual Integration Fixes	
Electronic Signature	
Sign Data Files	
Multiple File Sign	
Multiple File Revoke	
Sequences	

Table 6-1 Enterprise Options Dialog (continued)

Project Name	**User**
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	
Advanced Reports	
Open Advanced Report	
Save Advanced Report	
Instrument Activity Log	
Purge Activity Log	
Security	
Access Common Folder	
Notes	

Table 6-1 Enterprise Options Dialog (continued)

Project Name	User

Table 6-2 User, Instrument Administrator, and System Administrator

User	Instrument Administrator	System Administrator
	□	□
	□	□
	□	□
	□	□
	□	□
	□	□
	□	□
	□	□
	□	□
	□	□

Table 6-3 System and User Assignment

System	User	User	User

Table 6-3 System and User Assignment (continued)

System	User	User	User

Contact Us

Customer Training

- In North America: NA.CustomerTraining@sciex.com
- In Europe: Europe.CustomerTraining@sciex.com
- Outside the EU and North America, visit sciex.com/education for contact information.

Online Learning Center

- SCIEX Now Learning Hub

Purchase Supplies and Reagents

Reorder SCIEX supplies and reagents online at store.sciex.com. To set up an order, use the account number, found on the quote, order confirmation, or shipping documents. Currently, customers in the United States, United Kingdom, and Germany have access to the online store, but access will be extended to other countries in the future. For customers in other countries, contact a local SCIEX representative.

SCIEX Support

SCIEX and its representatives maintain a staff of fully-trained service and technical specialists located throughout the world. They can answer questions about the system or any technical issues that might arise. For more information, visit the SCIEX website at sciex.com or contact us in one of the following ways:

- sciex.com/contact-us
- sciex.com/request-support

CyberSecurity

For the latest guidance on cybersecurity for SCIEX products, visit sciex.com/productsecurity.

Documentation

This version of the document supercedes all previous versions of this document.

To view this document electronically, Adobe Acrobat Reader is required. To download the latest version, go to https://get.adobe.com/reader.

Contact Us

To find software product documentation, refer to the release notes or software installation guide that comes with the software.

To find hardware product documentation, refer to the documentation DVD for the system or component.

The latest versions of the documentation are available on the SCIEX website, at sciex.com/customer-documents.

Note: To request a free, printed version of this document, contact sciex.com/contact-us.