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 operating 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.

© 2019 AB Sciex
CHAPTER 1

32 Karat Enterprise Overview

⚠️ CAUTION

Prior to using the system, refer to the safety content in the System Overview Guide for detailed information on the safe use and operation of the system.

The SCIEX P/ACE™ MDQ Plus software includes the 32 Karat software. System Administration of instruments and users is done through the 32 Karat Enterprise window. For the proper functioning of the P/ACE™ MDQ Plus software, SCIEX strongly recommends you enable the System Administration option. To do this, click **Tools > Options > Enterprise** and then select **Enable user logins and permissions**.

After these settings are enabled, each user must log in. This feature helps to ensure data integrity and system security.

**Enterprise Window**

When the P/ACE™ MDQ Plus software is launched, the Enterprise window appears.
The Enterprise window manages the following:

- Instruments—data acquisition and analysis
- Projects—specially identified sets of folders
- System Administration—user privileges and security

**System Administration**

System Administration supplies the tools to manage account and user privileges and security. When the 32 Karat software is installed, security features are disabled and the Enterprise window contains the following users, groups, instruments, and projects:

- **User:** mdq
- **Password:** plus
- **Group:** Analysis
- **Sub-Group:** UV
- **Instrument - Project - UV**

In System Administration, different types of users are designated along with limits to their access and control. The limit to the number of users that have access to the P/ACE™ MDQ Plus and to the 32 Karat software is also configured in System Administration.

For the proper functioning of the P/ACE™ MDQ Plus software, all instruments defined should have a project defined that is named exactly the same. The P/ACE™ MDQ Plus software associates like project names with like instrument names to simplify the user experience.
System Administration Workflow

This guide uses the following sequence for system setup:

1. Create System Administrator
2. Add Users
3. Create Projects
4. Assign Instrument Administrator
5. Assign User Privileges
6. Create Instruments
7. Grant User Access to Instruments

System Administration Wizard

The System Administration Wizard and options in the Tools menu are active to enable setup of the above-listed features.

User Types

The 32 Karat software has three different types of users:

- System Administrator
- Instrument Administrator
- User

System Administrator

The System Administrator can use all functions in the software, as well as manage the following:

- Enable login
- Manage project settings
- Add/Remove user access to the 32 Karat software and to the P/ACE™ MDQ Plus software
- Assign instrument or instrument administrator responsibility to users
- Manage project privileges for each user

Instrument Administrator

The Instrument Administrator is limited to configuring instruments:

- Managing instruments (add, delete, rename, or configure)
- Granting user access to instruments
User

The user is limited to the specific Instruments and Projects as specified by the Administration Policies set by the Instrument and System Administrator.

User Locations

The 32 Karat Enterprise software administers user names and passwords. If the controller is connected to a network, user names can be selected from a domain. The password is inherited from the domain and subject to all of the domain password limits.

NOTE As installed, the 32 Karat software has one default user: mdq. This account has system and instrumentation administration privileges.
CHAPTER 2
Getting Started

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.

Setting the Login Option

When login is enabled, a valid user name and password must be entered to access instrument or administration features.

1. Double-click the 32 Karat software icon to open the Enterprise window.

2. Click Tools.

3. To verify that the System administration mode is enabled, check to see if Enterprise Logout is displayed under the Tools menu. If it is not, click Enterprise Logout and log in as “mdq” using the password “plus”.

   IMPORTANT The Options dialog appears as different tabs depending on whether a valid System Administrator is logged in.

   - If Enterprise Logout is not shown, the Enterprise tab on the Options dialog is not visible.
   - If no System Administrator has been selected, the Enterprise tab on the Options dialog will be visible.
   - If a System Administrator has already been selected, the System Administrator user name and password must be entered to enable System Administration.

4. Click Tools > Options.
5  Click the Enterprise tab.

6  Click Enable user logins and permissions.

Data System User Passwords

Adding users to the data system requires entry and confirmation of user passwords. If a high level of security is not required, the System Administrator can allow the system to save user passwords after the first login. These passwords will stay in the 32 Karat software memory until the 32 Karat software is closed.

A data system user may change their password at any time by clicking Tools > Change Password.

IMPORTANT Domain user passwords are managed according to Network Administration policies.

Using the Networked Domain

If the system is connected to a network, users can be selected from a specified domain. This can provide a greater degree of security, because passwords are inherited from the network domain.

As with data system users, the System Administrator can limit access to only one domain user at a time. If this feature is enabled, the System Administrator can also specify this user as the current domain user (the user currently logged on to the network at the P/ACE™ MDQ Plus controller).

Selecting a User from a Network Domain

Identify the name of the network domain that contains the names of the users to be added.

NOTE Adding Domain Users may require assistance from your Network Administrator.

1  Open My Network Places on the Desktop to search for nearby domain names.

2  Click Entire Network. This option will display all of the available domains.

3  Click Tools > Options > Enterprise tab and Enable Login from the Enterprise window.
4 Click **Domain controller**.

5 Click **Add Domain**.

6 Type the name of the domain in the entry field and then click **Save**.

**Figure 2.1** Domain Information Dialog

7 Click **Apply**, then click **OK**.

---

**Designating the System Administrator from the Domain**

Since there is no System Administrator selected yet, log back in and select a domain name as the System Administrator.

1 Click **Tools > Enterprise login**. A list of all users (and groups of users) from the specified domain will be displayed.

**Figure 2.2** Select System Administrator Dialog
2 Enter a user or group name and click **Check Names**. If the name is found, the down arrow turns green. Select the valid name and the green arrow to move the name into the Selected user group. Click **OK**. A login dialog appears to confirm the System Administrator’s user name and password.

3 Enter the network user name and password to continue in System Administration Mode.

### Additional Security

The 32 Karat software provides additional security to domain user accounts by adding options for Logout.

1 Click **Tools > Options**, then select **General** tab.

2 Click the option to **log out the current user when idle for**: Enter the time out desired in minutes.

3 Click the **E-mail** tab and fill in the required fields. You may need a network administrator to help you with the information required.

4 Click **OK**.

### Selecting a System Administrator from the Data System

If a domain controller is not desired for logging in, you can use the Data System on the local P/ACE™ MDQ Plus controller.

1 Click **Tools > Options**, then **Enterprise**.

2 Click **Enable Login**.

3 Click **Data System**.

4 Click **Add User**.
5 Enter the user name and password for the System Administrator and click Save.

6 Click Save > Apply, then select OK.

7 Click Tools > Enterprise login.

8 Click Tools > System Administration Wizard.

9 Click User, then select Next.

10 Select the user to be specified as the System Administrator and click Next.

11 Click the option for System Administration and click Finish.
   More System Administrator Wizard features are described in System Administration Wizard on page 15.

12 Click Tools > Enterprise Logout, then log in by clicking Tools > Enterprise Login.

13 Enter the user name and password for the user, then log in as the System Administrator.

NOTE The System Administrator name displays in the lower-left corner of the Enterprise window.

Figure 2.3 Enterprise Window Depicting System Administrator Login
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.

**Adding Projects**

After entering users, the System Administrator must specify project access for each user.

1. Click **Tools > System Administration Wizard**.

2. Click **Project**.

3. Click **Next**.

4. Click **Create a new project**.

5. Click **Next** to enter the **General Project Settings**.

6. Enter a new project name in **Name**.

   This name will be assigned to a Windows folder that the 32 Karat software identifies as a project. The default path for all projects is `C:\32Karat\Projects`, but a different path can be specified.

   **NOTE**  Subfolders for this project will be automatically created.
Additional Project Settings

1. Click Next to specify audit trails for this project.
   Method and sequence audit trails can be enabled individually as they are created, or they can be made active automatically in the project as specified in this dialog.

2. Click Next to define the Electronic Signature roles. These roles explain what each user signature means for a given data file (refer to Electronic Signature on page 21).

3. Click Next to specify the users that will have access to this project.
Select Users

This setting describes the features each user can access in each project.

1. Click one or more users from the **Available Users** column. Use the **SHIFT** key to select multiple contiguous users, or the **CTRL** key to select multiple non-contiguous users. Use the arrow keys in the center to move users between the Available and Selected users.

2. Click **Next** to assign user privileges.

3. Click one or more users from the **Selected Users** list (use the **SHIFT** or **CTRL** key to select multiple users, or **CTRL+A** to select all users). Next select from the Unassigned privileges list (use the **SHIFT** or **CTRL** key to select multiple privileges, or **CTRL+A** to select all privileges), then use the arrow key to move them to the **Assigned** privileges.

   See **User Privileges on page 31** for a complete list of user privileges. When options listed in the left pane are transferred to the right pane, they become assigned privileges for the selected users. This means a user has the right to use the specified feature in this project.

4. Click **Next** to set the user Electronic Signature Role.

User Electronic Signature Roles

As described above, the electronic signature roles for each project can be uniquely specified. If a user has been granted access to this option, the electronic signature role of the user must be set (refer to **Electronic Signature on page 21**).

After assigning electronic signature roles, click **Finish**.

Additional User Settings

The System Administrator may also designate another user as a System Administrator or an Instrument Administrator.

**NOTE** An Instrument Administrator is responsible for adding and configuring instruments.

1. Click **Tools > System Administration Wizard**.

2. Click **User**.
3 Click Next.

4 Click the user you want to grant System Administrator privileges.

5 Click System Administration or Instrument Administration.

NOTE In some cases, the Instrument Administrator may be the same user as the System Administrator.

6 Click Finish.

NOTE Make sure that at least one user is designated as a System Administrator and at least one user is designated as an Instrument Administrator.

7 Click Tools > Enterprise Logout.
CHAPTER 4

Using the 32 Karat Software Under System Administration

Creating New Instruments

With a new P/ACETM MDQ Plus system, one instrument is installed. Only an Instrument Administrator can create new instruments.

Instrument Administration Login

The Instrument Administrator must first log into the Enterprise by clicking Enterprise Login from the Tools menu. After the Instrument Administrator enters the correct user name and password, the login dialog indicates the user name and instrument administration mode in the bottom right corner of the active dialog.

Figure 4.1 User Name and Instrument Administration Mode

Create and configure instruments as instructed in the online help. With instruments present and configured, give access to the users.

Setting User Access to Instruments

By Instrument Administrator

An Instrument Administrator can grant instrument access to existing users by right-clicking on the instrument and clicking Add/Modify Users.

Double-click a user name to add users from the list on the left, or select and use the arrow buttons in the center to move users between Available and Selected users for the instrument.
By System Administrator

The System Administrator can also provide instrument access to a user from the System Administration Wizard.

1. Click **Tools > Enterprise Login**. Enter the user name and password and click **Login**.

2. Click **Tools > System Administration Wizard**. Click **User** and click **Restart selected wizard when finished**.

3. Click **Next**.

4. Select a User.

5. Click **Next**.

6. Modify Administration privileges and click **Next**. Select instruments and use the arrow buttons in the center to assign instrument access to users.

7. Click **Finish**.

8. Repeat steps 4 through 7 for each additional user. Click **Cancel** to close the wizard.
CHAPTER 5
Additional Features

Electronic Signature

Electronic Signature features are set by the System Administrator and allow the user to acquire, review and 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. Click Tools > System Administration Wizard.

2. Click Project, then click Next.

3. Click Change a project's settings, then click Next.

4. Click the project, then click Next.

5. Click Next, modify audit trail settings, then click Next.

6. Define the Electronic Signature Roles applicable to the selected project. Click Finish or Next to modify any other settings for the project.
**Figure 5.1 Define Electronic Signature Roles Dialog**

![Define Electronic Signature Roles](image)

**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 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 5.2**  Modify Electronic Signature Reasons Dialog

![Modify Electronic Signature Reasons Dialog](image)

**Global Options**

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

**NOTE**  SCIEX recommends that you enable Extended security and click Enable system activity log.
Figure 5.3 Options Dialog, Showing Logging and Extended Security Options

**System Activity Log**

This section describes working with the System Activity Log.

1. To view the current System Activity Log, go to the **Main** menu.

2. Click **File > System Activity Log > Display Log**.
   The current system activity log appears.

3. Right-click in the table for a menu used to access the functions of the System Activity Log.
   This menu is disabled unless the user has System Administration or Instrument Administration rights assigned.
Table 5.1  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

Place a manual entry into the system activity log.

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

Figure 5.5  System Activity Log 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 5.2  System Activity Log for Selected Record Ranges

<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, click File > System Activity Log > Archive from the Main menu. A dialog appears 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 that is run from the 32 Karat program group in Windows. (From the Windows task bar, click Start > All Programs > P/ACE MDQ plus Software > Log Viewer.)

Figure 5.6  Start the P/ACE™ MDQ Plus Software Log Viewer

Purge

To purge the System Activity Log, click File > System Activity Log > Purge.

- 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, click 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 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.

**Initial Setup of Users, Projects, Instruments, and Settings**

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

Refer to Adding Projects on page 15 for setup instructions.
System Projects

The lab manager will create the following projects:

- Protein
- Nucleic Acid
- Small Molecules
- Performance

Refer to Adding Projects on page 15 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

Refer to Additional Project Settings on page 16 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

Refer to User Electronic Signature Roles on page 17 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

Refer to Creating New Instruments on page 19 for setup instructions.

Adding a New User

At this point, the Lab Manager decides to hire a biostatistician. 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 clicks **Enterprise login** from the **Tools** menu and enters the appropriate user name and password.

2 LabMgr clicks **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 clicks **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 A.1 User Project Privileges Worksheet

<table>
<thead>
<tr>
<th>Project Name</th>
<th>User</th>
<th>User</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Methods</strong></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><strong>Data</strong></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><strong>Electronic Signature</strong></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>
</tbody>
</table>
### Table A.1  User Project Privileges Worksheet (Continued)

<table>
<thead>
<tr>
<th>Project Name</th>
<th>User</th>
<th>User</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequences</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Sequence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save Sequence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preview Run</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single Run</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sequence Run</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock Instrument</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Print Setup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual Control (Idle Only)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pretreatment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Pretreat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save Pretreat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Reports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Advanced Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save Advanced Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instrument Activity Log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purge Activity Log</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Common Folder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tune</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Tune</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Save Tune</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Tune</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calibration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table A.2  User Administrator Privileges Worksheet

<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>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table A.3  User Instrument Privileges Worksheet

<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>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

- SCIEXUniversity

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 supersedes 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.

To find software product documentation, refer to the release notes or software installation guide that comes with the software. Documentation for the hardware products can be found on the Customer Reference DVD that comes with the system or component.

For the latest versions of the documentation, visit the SCIEX website at sciex.com.

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