SCIEX

The Power of Precision

SCIEX OS Software

Laboratory Director Guide

RUO-IDV-05-7370-H

November 2021

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

Contents

Contents

Introduction 1

The information contained in this manual is intended for two primary audiences:

- The laboratory administrator, who is concerned with the daily operation and use of the SCIEX OS software and attached instrumentation from a functional perspective.
- The system administrator, who is concerned with system security and system and data integrity.

Security Configuration Overview 2

This section describes how SCIEX OS access control and auditing components work in conjunction with Windows access control and auditing components. It also describes how to configure Windows security before installing SCIEX OS.

Security and Regulatory Compliance

SCIEX OS provides:

- Customizable administration to meet the needs of both research and regulatory requirements.
- Security and audit tools to support 21 CFR Part 11 compliance for the use of electronic record keeping.
- Flexible and effective management of access to critical mass spectrometer functions.
- Controlled and audited access to vital data and reports.
- Easy security management linking to Windows security.

Security Requirements

Security requirements range from relatively open environments, such as research or academic laboratories, to the most stringently regulated, such as forensic laboratories.

SCIEX OS and Windows Security: Working Together

SCIEX OS and the Windows New Technology File System (NTFS) have security features designed to control system and data access.

Windows security provides the first level of protection by requiring users to log on to the network using a unique user identity and password. As a result, only users who are recognized by the Windows Local or Network security settings have access to the system. For more information, refer to the section: Windows Security Configuration.

SCIEX OS has the following secure system access modes:

- Mixed mode
- Integrated mode (default setting)

For more information about security modes and security settings, refer to the section: Configure the Security Mode.

SCIEX OS also provides completely configurable roles that are separate from the user groups associated with Windows. By using roles, the laboratory director can control access to the software and mass spectrometer on a function-by-function basis. For more information, refer to the section: Configure Access to SCIEX OS.

Audit Trails within SCIEX OS and Windows

The auditing features within SCIEX OS, together with the built-in Windows auditing components, are critical to the creation and management of electronic records.

SCIEX OS provides a system of audit trails to meet the requirements of electronic record-keeping. Separate audit trails record:

- Changes to the mass calibration table or resolution table, system configuration changes, and security events.
- Creation and modification events for projects, tuning, batches, data, processing methods, and report template files, as well as module opening, closing, and printing events. Deletion events recorded in the audit trail include deletion of roles and deletion of users in SCIEX OS.
- Creation and modification of the sample information, peak integration parameters, and embedded processing method in a Results Table.

Note: SCIEX OS does not audit creation of or changes to MS methods, LC methods, batches, or processing methods. These files act as templates. Parameter values are read from them at the time of acquisition or processing, and applied to the task. For MS methods, LC methods, and batches, the parameter values are recorded in the wiff and wiff2 files. For processing methods, they are recorded in the qsession file. These files serve as the electronic records for this information.

For a complete list of audit events, refer to the section: Audit Events.

SCIEX OS uses the application event log to capture information about software operation. Use this log as a troubleshooting aid. It contains detailed information about mass spectrometer, device, and software interactions.

Windows maintains event logs, which capture a range of security-, system-, and application-related events. In most cases, Windows auditing is designed to capture exceptional events, such as a log on failure. The administrator can configure this system to capture a wide range of events, such as access to specific files or Windows administrative activities. For more information, refer to the section: System Audits.

21 CFR Part 11

SCIEX OS contains the technical controls to support 21 CFR Part 11 with the implementation of:

- Mixed mode and Integrated mode security linked to Windows security.
- Controlled access to functionality through customizable roles.
- Audit trails for instrument operation, data acquisition, data review, and report generation.
- Electronic signatures that use a combination of user ID and password.
- Proper configuration of the Windows operating system.
- Proper procedures and training in the company.

SCIEX OS is designed to be used as part of a 21 CFR Part 11-compliant system and can be configured to support 21 CFR Part 11 compliance. Whether the use of SCIEX OS is 21 CFR Part 11-compliant depends on the actual usage and configuration of SCIEX OS in the lab.

Validation services are available through SCIEX Professional Services. For more information, contact complianceservices@sciex.com.

Note: Do not leave the Instrument Settings Converter software on a validated system. It is intended for the initial transfer of instrument settings from the Analyst software to SCIEX OS. Make sure to remove the Instrument Settings Converter software from the computer after using it.

System Configuration

System configuration is usually performed by network administrators or people with network and local administration rights.

Windows Security Configuration

The system implements the following restrictions for the local Windows user accounts:

- The Windows password must be changed every 90 days.
- The Windows password cannot be reused for at least one following iteration. That is, it cannot be the same as previous password.
- The Windows password must be a minimum of eight characters.
- The Windows password must contain at least two of the following four requirements to meet complexity requirements:
  - One upper case alpha character
  - One lower case alpha character
  - One numeric value
  - One special character (such as: ! @ # $ % ^ &)

- The Windows user name must not be **admin**, **administrator**, or **demo**.

The SCIEX OS administrator must have the ability to change file permissions for the SCIEX OS Data folder. If this folder is on a local computer, then we suggest that the software administrator be part of the local administrators group.

To make sure that all users have the required access to resources for network acquisition, the network administrator can define a Secure Network Account (SNA) on the network resource. This account must have write permissions for the network folder containing the root directory. It is defined as the SNA in the properties for the root directory.

Users and Groups

SCIEX OS uses the user names and passwords recorded in the primary domain controller security database or Active Directory. Passwords are managed using the tools provided with Windows. For more information about adding and configuring people and roles, refer to the section: Configure Access to SCIEX OS.

Active Directory Support

When adding users in the SCIEX OS Configuration workspace, specify user accounts in user principal name (UPN) format. The following versions of Active Directory are supported:

- Windows 2012 servers.
- Windows 7, 64-bit clients
- Windows 10, 64-bit clients

Windows File System

In SCIEX OS, files and directories must be stored on a hard-disk partition that uses the NTFS format, which can control and audit access to SCIEX OS files. The File Allocation Table (FAT) file system cannot control or audit access to folders or files and is, therefore, not suitable for a secure environment.

File and Folder Permissions

To manage security, the SCIEX OS administrator must have the right to change permissions for the SCIEX OS Data folder. Access must be set up by the network administrator.

Note: Consider the level of access users need to the drive, root directory, and project folders on each computer. Configure sharing and associated permissions. For more information about file sharing, refer to the Windows documentation.

For information about the SCIEX OS files and folder permissions, refer to the section: Access Control.

System Audits

The auditing feature of the Windows system can be enabled to detect security breaches or system intrusions. Auditing can be set to record different types of system-related events. For example, the auditing feature can be enabled to record any failed or successful attempt to log on to the system in the event log.

Event Logs

The Windows Event Viewer records the audited events in the security log, system log, or application log.

Customize the event logs as follows:

- Configure an appropriate event log size.
- Enable automatic overwrite of old events.
- Set Windows computer security settings.

A process of review and storage can be implemented. For more information about security settings and audit policies, refer to the Windows documentation.

Windows Alerts

If a system or user issue occurs, then configure the network to send an automatic message to a designated person, such as the system administrator, on the same computer or another computer.

- On both the sending and receiving computer, start the Messenger in the Windows Services control panel.
- On the sending computer, start the Alert service in the Windows Services control panel.

For more information about creating an alert object, refer to the Windows documentation.

Electronic Licensing 3

Electronic licensing can be node-locked or server-based.

The Activation ID might be required for any future service or support call. To access the Activation ID of the node-locked or server-based license:

- In the Configuration workspace, click **Licenses** in the SCIEX OS window.

Note: Make sure to renew the license before it expires.

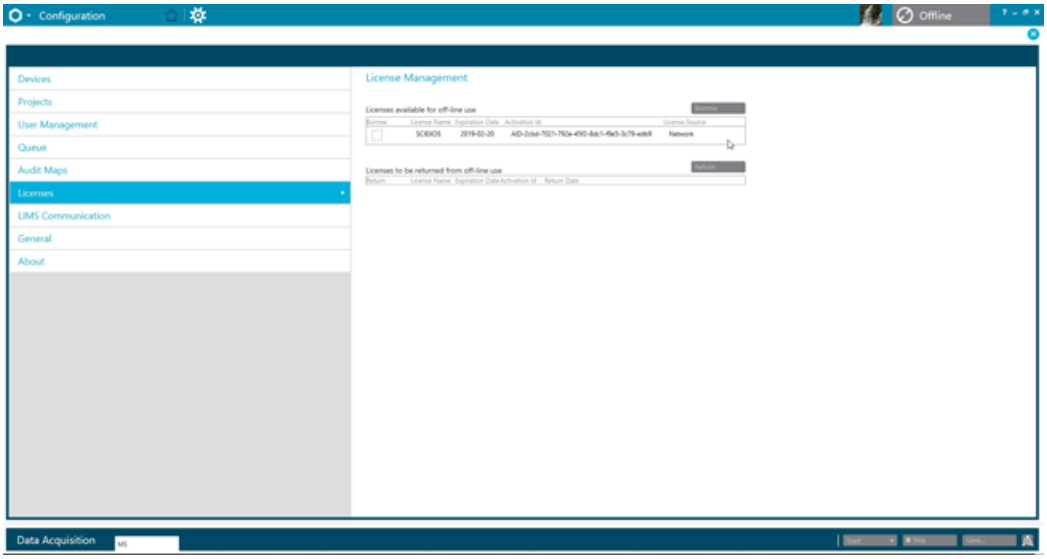
Borrow a Server-based Electronic License

A license is required to use SCIEX OS. If server-based licensing is being used, then users who want to work offline can reserve a license for up to 7 days. During this period, the borrowed electronic license is dedicated to the computer.

1. Open the Configuration workspace.
2. Click **Licenses**.

   The Licenses available for off-line use table shows all licenses available for borrowing.

Figure 3-1 License Management: Borrow a License



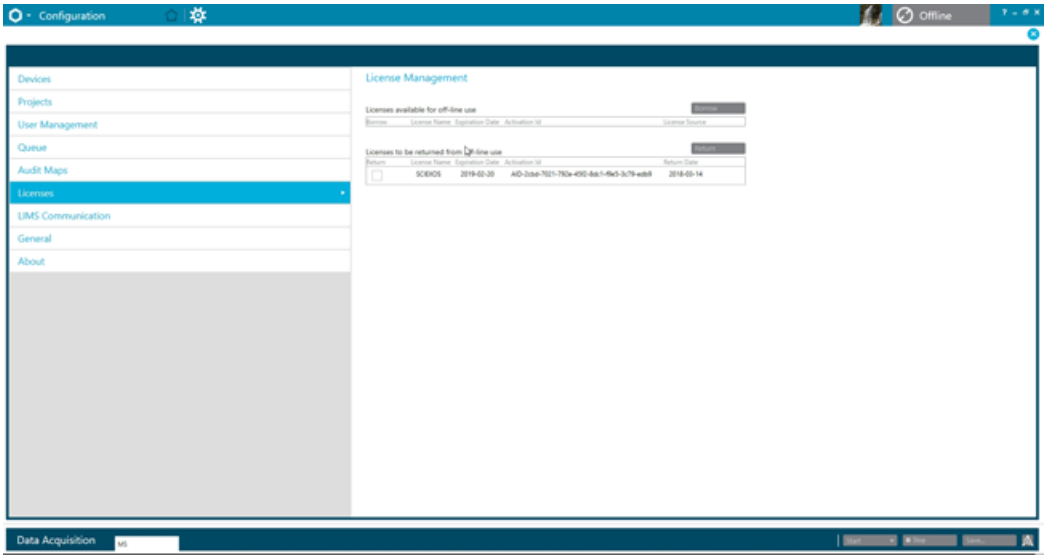
3. Select the license to be borrowed, and then click **Borrow**.

Return a Server-based Electronic License

1. Open the Configuration workspace.
2. Click **Licenses**.

   The Licenses to be returned from off-line use table shows all of the licenses that are eligible to be returned, that is, all licenses borrowed by this computer.

Figure 3-2 License Management: Return a License



3. Select the license to be returned, and then click **Return**.

Access Control 4

This section describes how to control access to SCIEX OS. To control access to SCIEX OS, the administrator performs the following tasks:

Note: To perform the tasks in this section, the user must have local administrator privileges for the workstation on which the software is being installed.

- Install and configure SCIEX OS.
- Add and configure users and roles.
- Configure access to the projects and project files in the root directory.

Note: Any changes to the SCIEX OS configuration take effect after SCIEX OS is restarted.

Location of Security Information

All security information is stored on the local computer, in the C:\ProgramData\SCIEX\Clearcore2.Acquisition folder, in a file named Security.data.

Software Security Workflow

SCIEX OS works with the security, application, and system event auditing components of the Windows Administrative Tools.

Configure security at the following levels:

- Windows authentication: Access to the computer.
- Windows authorization: Access to files and folders.
- SCIEX OS authentication: Ability to open SCIEX OS.
- SCIEX OS authorization: Access to functionality in SCIEX OS.

For the list of tasks for configuring security, refer to the table: Table 4-1. For the options for setting the various security levels, refer to the table: Table 4-2.

Table 4-1 Workflow Process for Configuring Security

Task	Procedure
Install SCIEX OS.	Refer to the document: *SCIEX OS Software Installation Guide*.
Configure access to SCIEX OS.	Refer to the section: Configure Access to SCIEX OS.
Configure Windows File Security and NTFS.	Refer to the section: Configure Access to Projects and Project Files.

Table 4-2 Security Configuration Options

Option	CFR 21 Part 11
Windows Security	
Configure users and groups (authentication).	Yes
Enable Windows auditing and file and directory auditing.	Yes
Set file permissions (authorization).	Yes
SCIEX OS Installation	
Install SCIEX OS.	Yes
Open the Event Viewer to inspect the installation.	Yes
Software Security	
Select the security mode.	Yes
Configure SCIEX OS users and roles.	Yes
Configure email notification.	Yes
Create audit map templates, and configure project and workstation audit trail maps.	Yes
Enable the checksum feature for wiff files.	Yes
Common Tasks	
Add new projects.	Yes

Install SCIEX OS

Before installing SCIEX OS, read these documents, available on the software installation DVD: *Software Installation Guide* and *Release Notes*. Be sure to understand the difference between a processing computer and an acquisition computer and then complete the appropriate installation sequence.

System Requirements

For minimum installation requirements, refer to the document: *Software Installation Guide*.

Preset Auditing Options

For a description of the installed audit maps, refer to the section: Installed Audit Map Templates. After installation, the SCIEX OS administrator can create custom audit maps and assign a different audit map in the Configuration workspace.

Configure the Security Mode

This section describes the Security Mode options found on the User Management page in the Configuration workspace.

Integrated Mode: If the user who is currently logged on to Windows is defined as a user in SCIEX OS, then that user has access to SCIEX OS.

Mixed Mode: Users log on to Windows and SCIEX OS separately. The credentials used to log on to Windows need not be the same as the credentials used to log on to SCIEX OS. Use this mode to allow a group of users to log on to Windows with the same set of credentials, but require each user to log on to SCIEX OS with unique credentials. These unique credentials can be assigned to a specified role in the same way as in Integrated mode.

If Mixed mode is selected, then the Screen Lock and Auto Logoff features are available for use.

Screen Lock and Auto Logoff: For security purposes, the computer screen can be set to lock after a defined period of inactivity. An automatic logoff timer can also be set, so that SCIEX OS closes after it has been locked for a defined period. Screen Lock and Auto Logoff are available in Mixed mode only.

Note: When the screen locks, acquisition and processing continue. Automatic logoff will not occur if processing is occurring or if the Results Table has not been saved. When the user is logged off using the forced log off, all processing stops, and all unsaved data is lost. Acquisition continues after the user is logged off, either automatically or manually.

Security Notification: The software can be configured to automatically send an e-mail notification after a configurable number of logon failures within a configurable period, to warn of attempts to

access the system by unauthorized users. The number of logon failures can be from 3 to 7, and the period can be from 5 minutes to 24 hours.

Select the Security Mode

1. Open the Configuration workspace.
2. Click **User Management**.
3. Click the **Security Mode** tab.
4. Select **Integrated Mode** or **Mixed Mode**. Refer to the section: Configure the Security Mode.
5. Click **Save**.

   A confirmation dialog is shown.
6. Click **OK**.

Configure Workstation Security Options (Mixed Mode)

Prerequisite Procedures
• Set the security mode to Mixed mode. Refer to the section: Configure the Security Mode.

If Mixed mode is selected, then the Screen Lock and Auto Logoff features can be configured.

1. Open the Configuration workspace.
2. Click **User Management**.
3. Open the Security Mode tab.
4. To configure the Screen Lock feature, follow these steps:
   a. Select **Screen Lock**.
   b. In the **Wait** field, specify a time, in minutes.

      If the workstation is inactive for this amount of time, then it is automatically locked. The logged-on user can unlock the workstation by entering the correct credentials, or the Administrator can log the user off.
5. To configure the Auto Logoff feature, follow these steps:
   a. Select **Auto Logoff**.
   b. In the **Wait** field, specify a time, in minutes. If the workstation is locked for this amount of time, either automatically or manually, then the currently logged on user is logged off. All processing stops. Acquisition, however, continues.
6. Click **Save**.

A confirmation dialog box opens.

7. Click **OK**.

Configure E-mail Notification (Mixed Mode)

Prerequisite Procedures
• Set the security mode to Mixed mode. Refer to the section: Configure the Security Mode.

SCIEX OS can be configured to send an e-mail message after a configurable number of logon errors within a configurable period. The number of logon failures can be from 3 to 7, and the period from 5 minutes to 24 hours.

The computer with SCIEX OS must be able to communicate with an SMTP server with an open port.

1. Open the Configuration workspace.
2. Click **User Management**.
3. Open the Security Mode tab.
4. Select the **Send e-mail messages after** check box and then specify how many logon failures within what period, in minutes, will generate an e-mail notification.

   Tip! To disable notification, clear the **Send e-mail messages after** check box.

5. In the **SMTP Server** field, type the name of the SMTP server.

   Note: The SMTP account sends mail to the e-mail server. The SMTP server is defined in the corporate e-mail application.

6. In the **Port Number** field, type the number of the open port.

   Click **Apply Default** to insert the default port number, 25.

7. In the **To** field, type the e-mail address to which the message is to be sent. For example: username@domain.com.
8. In the **From** field, type the e-mail address to be shown in the **From** field of the message.
9. In the **Subject** field, type the subject of the message.
10. In the **Message** field, type the text to be included in the body of the message.
11. Click **Save**.

    A confirmation dialog opens.

12. Click **OK**.

13. To check the configuration, click **Send Test Mail**.

Configure Access to SCIEX OS

Before configuring security, do the following:

- Remove all of the unnecessary users and user groups, such as replicator, power user, and backup operator, from the local computer and the network.

  Note: Every SCIEX computer is configured with a local Administrator-level account, **abservice**. This account is used by SCIEX service and technical support to install, service, and support the system. Do not remove or deactivate this account. If the account must be removed or deactivated, then prepare an alternate plan for SCIEX access, and communicate it to the local FSE.

- Add user groups containing groups that will have non-administrative tasks.
- Configure system permissions.
- Create suitable procedures and account policies for the users in Group Policy.

Refer to the Windows documentation for more information about the following:

- Users and groups and Active Directory users.
- Password and account lockout policies for user accounts.
- User rights policy.

When users work in an Active Directory environment, the Active Directory group policy settings affect the computer security. Discuss group policies with the Active Directory administrator as part of a comprehensive SCIEX OS deployment.

SCIEX OS Permissions

Figure 4-1 User Management Page

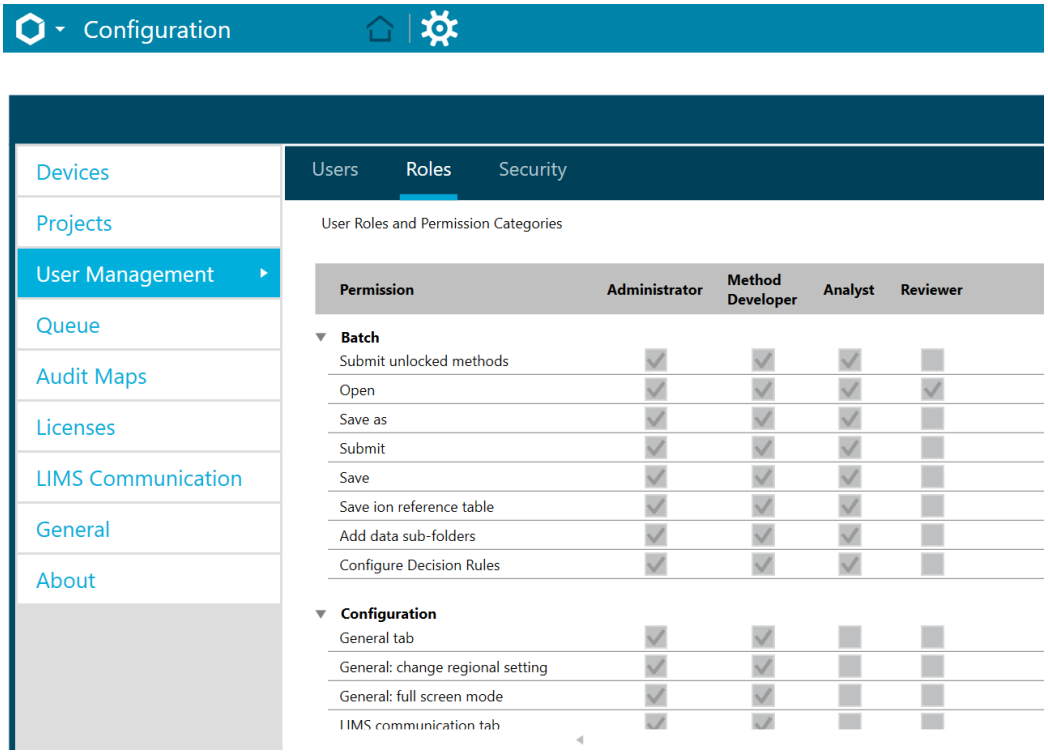


Table 4-3 Permissions

Permission	Description
Batch	
Submit unlocked methods	Allows users to submit batches that contain unlocked methods.
Open	Allows users to open existing batches.
Save as	Allows users to save batches with a new name.
Submit	Allows users to submit batches.
Save	Allows users to save a batch, overwriting the existing content.
Save ion reference table	Allows users to edit the ion reference table.
Add data sub-folders	Allows users to create subfolders to store data.
Configure Decision Rules	Allows users to add and change decision rules.

Table 4-3 Permissions (continued)

Permission	Description
Configuration	
General tab	Allows users to open the General page in the Configuration workspace.
General: change regional setting	Allows users to apply current system regional settings to SCIEX OS.
General: full screen mode	Allows users to enable and disable Full Screen mode.
LIMS communication tab	Allows users to open the LIMS Communication page in the Configuration workspace.
Audit maps tab	Allows users to open the Audit Maps page in the Configuration workspace.
Queue tab	Allows users to open the Queue page in the Configuration workspace.
Queue: instrument idle time	Allows users to set the instrument idle time.
Queue: max number of acquired samples	Allows users to set the maximum number of acquired samples allowed.
Queue: other queue settings	Allows users to configure other queue settings.
Projects tab	Allows users to open the Projects page in the Configuration workspace.
Projects: create project	Allows users to create projects.
Projects: apply an audit map template to an existing project	Allows users to apply an audit map to a project.
Projects: create root directory	Allows users to create a root directory to store projects.
Projects: set current root directory	Allows users to change the root directory for a project.
Projects: specify network credentials	Allows users to specify a secure network account (SNA) to be used during network acquisition if the logged-on user does not have access to the network resource.
Projects: Enable checksum writing for wiff data creation	Allows users to configure the software to write checksums to wiff data files.
Projects: clear root directory	Allows users to delete a root directory from the list.

Table 4-3 Permissions (continued)

Permission	Description
Devices tab	Allows users to open the Devices page in the Configuration workspace.
User management tab	Allows users to open the User Management page in the Configuration workspace.
Force user logoff	Allows users to force the log off of a user who is currently logged on to SCIEX OS.
Event Log	
Access event log workspace	Allows users to open the Event Log workspace.
Archive log	Allows users to archive the event log.
Audit Trail	
Access audit trail workspace	Allows users to open the Audit Trail workspace.
View active audit map	Allows users to view the active audit map for a workstation or project in the Audit Trail workspace.
Print/Export audit trail	Allows users to print or export the audit trail.
Data Acquisition Panel	
Start	Allows users to start acquisition in the Data Acquisition pane.
Stop	Allows users to stop acquisition in the Data Acquisition pane.
Save	Allows users to save acquired data with a different file name in the Data Acquisition pane.
MS & LC Method	
Access method workspace	Allows users to open the MS Method and LC Method workspaces.
New	Allows users to create MS and LC methods.
Open	Allows users to open MS and LC methods.
Save	Allows users to save a method, overwriting the existing content.
Save as	Allows users to save methods with a new name.
Lock/Unlock method	Allows users to lock methods, to prevent editing, and to unlock methods.
Queue	

Table 4-3 Permissions (continued)

Permission	Description
Manage	Allows users to open the Queue workspace.
Start/Stop	Allows users to start or stop the queue.
Print	Allows users to print the queue.
Library	
Access library workspace	Allows users to open the Library workspace. Not applicable to the Quantitation workflow.
MS Tune	
Access MS Tune workspace	Allows users to open the MS Tune workspace.
Advanced MS tuning	(X500 QTOF Systems) Allows users to access the advanced tuning options, including Detector Optimization, Positive and Negative Q1 Unit Tuning, Positive and Negative TOF MS Tuning, and Positive and Negative Q1 High Tuning.
Advanced troubleshooting	Allows users to open the Advanced Troubleshooting dialog.
Quick status check	(X500 QTOF Systems) Allows users to perform the Positive and Negative Quick Status Checks.
Restore instrument data	Allows users to restore previously saved tuning settings.
Explorer	
Access Explorer workspace	Allows users to open the Explorer workspace.
Export	Allows users to export data from the Explorer workspace.
Print	Allows users to print data in the Explorer workspace.
Options	Allows users to modify the options for the Explorer workspace.
Recalibrate	Allows users to recalibrate samples and spectra in the Explorer workspace. Not applicable to the Quantitation workflow.
Analytics	
New results	Allows users to create Results Tables.
Create processing method	Allows users to create processing methods.
Modify processing method	Allows users to modify processing methods.
Allow Export and Create Report of unlocked Results Table	Allows users to export or generate a report from a Results Table, if the Results Table is not locked.

Table 4-3 Permissions (continued)

Permission	Description
Save results for Automation Batch	Allows Results Tables created automatically in the Batch workspace to be saved.
Change default quantitation method integration algorithm	Allows users to change the integration algorithm in the project default settings.
Change default quantitation method integration parameters	Allows users to change the integration parameters in the project default settings.
Enable project modified peak warning	Allows users to enable the modified peak warning property for a project.
Project secure export settings	Allows users to change the secure export settings for a project.
Add samples	Allows users to add samples to a Results Table.
Remove selected samples	Allows users to remove samples from a Results Table.
Export, import, or remove external calibration	Allows users to export, import, or remove external calibrations.
Modify sample name	Allows users to modify the sample name in the Results Table.
Modify sample type	Allows users to modify the sample type, such as standard, quality control (QC), or unknown, in the Results Table.
Modify sample ID	Allows users to modify the sample ID in the Results Table.
Modify actual concentration	Allows users to modify the actual concentration of the standard and QC samples in the Results Table.
Modify dilution factor	Allows users to modify the dilution factor in the Results Table.
Modify comment fields	Allows users to modify comment fields: • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment
Enable manual integration	Allows users to perform manual integration.
Set peak to Not Found	Allows users to set a peak to **Not Found**.

Table 4-3 Permissions (continued)

Permission	Description
Include or exclude a peak from the Results Table	Allows users to include and exclude peaks from the Results Table.
Regression options	Allows users to change the regression options in the Calibration Curve pane.
Modify Results Table integration parameters for a single chromatogram	Allows users to change integration parameters for a single chromatogram in the Peak Review pane.
Modify quantitation method for the Results Table component	Allows users to select a different processing method for a component in the Peak Review pane with the **Update Processing Method for Component** option.
Create metric plot new settings	Allows users to create new Metric Plots and change the settings.
Add custom columns	Allows users to add custom columns to a Results Table.
Set peak review title format	Allows users to change the peak review title.
Remove custom column	Allows users to remove custom columns from a Results Table.
Results Table display settings	Allows users to customize the columns shown in the Results Table.
Lock Results Table	Allows users to lock a Results Table to prevent editing.
Unlock Results Table	Allows users to unlock a Results Table to allow editing.
Mark Results file as reviewed and save	Allows users to mark a Results Table as reviewed and save it.
Modify report template	Allows users to change report templates.
Transfer results to LIMS	Allows users to upload results to a Laboratory Information Management System (LIMS).
Modify barcode column	Allows users to change the **Barcode** column in a Results Table.
Change comparison sample assignment	Allows users to change the comparison sample specified in the **Comparison** column of the Results Table.
Add the MSMS spectra to library	Allows users to add the selected MS/MS spectra to a library. Not applicable to the Quantitation workflow.
Project default settings	Allows users to change the project default quantitative and qualitative processing settings.

Table 4-3 Permissions (continued)

Permission	Description
Create report in all formats	Allows users to generate reports in all formats. Users without this permission can only generate reports in PDF format.
Edit flagging criteria parameters	Allows users to change the flagging parameters in a processing method.
Automatic outlier removal parameter change	Allows users to change the parameters for automatic outlier removal.
Enable automatic outlier removal	Allows users to change the processing method to turn on the automatic outlier removal feature.
Update processing method via FF/LS	Allows users to update processing methods using Formula Finder and Library Search. Not applicable to the Quantitation workflow.
Update results via FF/LS	Allows users to update the results using Formula Finder and Library Search. Not applicable to the Quantitation workflow.
Enable grouping by adducts functionality	Allows users to update the processing method to turn on the grouping adducts feature.
Browse for files	Allows users to browse outside of the local data folder.
Enable standard addition	Allows users to update the processing method to turn on the standard addition feature.
Set Manual Integration Percentage Rule	Allows users to change the **Manual Integration %** parameter.

About Users and Roles

In SCIEX OS, the administrator can add Windows users and groups to the User Management database for SCIEX OS. To access the software, users must be defined in the User Management database, or must be a member of a group defined in the database.

Users can be assigned to one or more of the predefined roles, described in the following table, or to custom roles, if required. Roles determine the functions to which the user has access. The predefined roles cannot be deleted and their permissions cannot be modified.

Table 4-4 Predefined Roles

Role	Typical Tasks
Administrator	• Manages the system. • Configures security.
Method Developer	• Creates methods. • Runs batches. • Analyzes data for use by the end-user.
Analyst	• Runs batches. • Analyzes data for use by the end-user.
Reviewer	• Reviews data. • Reviews audit trails. • Reviews quantitation results.

Table 4-5 Preset Permissions

Permission	Administrator	Method Developer	Analyst	Reviewer
Batch				
Submit unlocked methods	✓	✓	✓	×
Open	✓	✓	✓	✓
Save as	✓	✓	✓	×
Submit	✓	✓	✓	×
Save	✓	✓	✓	×
Save ion reference table	✓	✓	✓	×
Add data sub-folders	✓	✓	✓	×
Configure Decision Rules	✓	✓	✓	×
Configuration				

Table 4-5 Preset Permissions (continued)

Permission	Administrator	Method Developer	Analyst	Reviewer
General tab	✓	✓	×	×
General: change regional setting	✓	✓	×	×
General: full screen mode	✓	✓	×	×
LIMS communication tab	✓	✓	×	×
Audit maps tab	✓	×	×	×
Queue tab	✓	✓	✓	✓
Queue: instrument idle time	✓	✓	×	×
Queue: max number of acquired samples	✓	✓	×	×
Queue: other queue settings	✓	✓	×	×
Projects tab	✓	✓	✓	✓
Projects: create project	✓	✓	✓	×
Projects: apply an audit map template to an existing project	✓	×	×	×
Projects: create root directory	✓	×	×	×
Projects: set current root directory	✓	×	×	×
Projects: specify network credentials	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation	✓	×	×	×
Projects: clear root directory	✓	×	×	×

Table 4-5 Preset Permissions (continued)

Permission	Administrator	Method Developer	Analyst	Reviewer
Devices tab	✓	✓	✓	×
User management tab	✓	×	×	×
Force user logoff	✓	×	×	×
Event Log				
Access event log workspace	✓	✓	✓	✓
Archive log	✓	✓	✓	✓
Audit Trail				
Access audit trail workspace	✓	✓	✓	✓
View active audit map	✓	✓	✓	✓
Print/Export audit trail	✓	✓	✓	✓
Data Acquisition Panel				
Start	✓	✓	✓	×
Stop	✓	✓	✓	×
Save	✓	✓	✓	×
MS & LC Method				
Access method workspace	✓	✓	✓	✓
New	✓	✓	×	×
Open	✓	✓	✓	✓
Save	✓	✓	×	×
Save as	✓	✓	×	×
Lock/Unlock method	✓	✓	×	×
Queue				
Manage	✓	✓	✓	×

Table 4-5 Preset Permissions (continued)

Permission	Administrator	Method Developer	Analyst	Reviewer
Start/Stop	✓	✓	✓	×
Print	✓	✓	✓	✓
Library				
Access library workspace	✓	✓	✓	✓
MS Tune				
Access MS Tune workspace	✓	✓	✓	×
Advanced MS Tuning	✓	✓	×	×
Advanced troubleshooting	✓	✓	×	×
Quick status check	✓	✓	✓	×
Restore instrument data	✓	✓	×	×
Explorer				
Access explorer workspace	✓	✓	✓	✓
Export	✓	✓	✓	×
Print	✓	✓	✓	×
Options	✓	✓	✓	×
Recalibrate	✓	✓	×	×
Analytics				
New results	✓	✓	✓	×
Create processing method	✓	✓	✓	×
Modify processing method	✓	✓	×	×

Table 4-5 Preset Permissions (continued)

Permission	Administrator	Method Developer	Analyst	Reviewer
Allow Export and Create Report of unlocked Results Table	✓	×	×	×
Save results for Automation Batch	✓	✓	✓	×
Change default quantitation method integration algorithm	✓	✓	×	×
Change default quantitation method integration parameters	✓	✓	×	×
Enable project modified peak warning	✓	×	×	×
Project secure export settings	✓	×	×	×
Add samples	✓	✓	✓	×
Remove selected samples	✓	✓	✓	×
Export, import, or remove external calibration	✓	✓	✓	×
Modify sample name	✓	✓	✓	×
Modify sample type	✓	✓	✓	×
Modify sample ID	✓	✓	✓	×
Modify actual concentration	✓	✓	✓	×
Modify dilution factor	✓	✓	✓	×
Modify comment fields	✓	✓	✓	×
Enable manual integration	✓	✓	✓	×

Table 4-5 Preset Permissions (continued)

Permission	Administrator	Method Developer	Analyst	Reviewer
Set peak to not found	✓	✓	✓	×
Include or exclude a peak from the results table	✓	✓	✓	×
Regression options	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram	✓	✓	✓	×
Modify quantitation method for the results table component	✓	✓	✓	×
Create metric plot new settings	✓	✓	✓	✓
Add custom columns	✓	✓	✓	×
Set peak review title format	✓	×	×	×
Remove custom column	✓	✓	×	×
Results table display settings	✓	✓	✓	✓
Lock results table	✓	✓	✓	✓
Unlock results table	✓	×	×	×
Mark results file as reviewed and save	✓	×	×	✓
Modify report template	✓	✓	×	×
Transfer results to LIMS	✓	✓	✓	×
Modify barcode column	✓	✓	×	×
Change comparison sample assignment	✓	✓	×	×

Table 4-5 Preset Permissions (continued)

Permission	Administrator	Method Developer	Analyst	Reviewer
Add the MSMS spectra to library	✓	✓	×	×
Project default settings	✓	✓	×	×
Create report in all formats	✓	✓	✓	✓
Edit flagging criteria parameters	✓	✓	✓	×
Automatic outlier removal parameter change	✓	✓	×	×
Enable automatic outlier removal	✓	✓	✓	×
Update processing method via FF/LS	✓	✓	×	×
Update results via FF/LS	✓	✓	×	×
Enable grouping by adducts functionality	✓	✓	×	×
Browse for files	✓	✓	✓	✓
Enable standard addition	✓	✓	✓	×
Set Manual Integration Percentage Rule	✓	×	×	×

Manage Users

Add a User or Group

1. Open the Configuration workspace.
2. Open the User Management page.
3. Open the Users tab.

4. Click **Add User** ().

   The Select User or Group dialog opens.

5. Type the name of a user or group and then click **OK**.

   Tip! For information about the Select User or Group dialog and how to use it, press **F1**.

6. To make the user active, make sure that the **Active user or group** check box is selected.
7. In the **Roles** area, select one or more roles, and then click **Save**.

Deactivate Users or Groups

1. Open the Configuration workspace.
2. Open the User Management page.
3. Open the Users tab.
4. In the **User name or group** list, select the user or group to be deactivated.
5. Clear the **Active user or group** check box.

   The system prompts for confirmation.

6. Click **Yes**.

Remove Users or Groups

Use this procedure to remove a user or group from the software. If a user or group is removed from Windows, then the user must also be removed from SCIEX OS.

1. Open the Configuration workspace.
2. Open the User Management page.
3. Open the Users tab.
4. In the **User name or group** list, select the user or group to be removed.
5. Click **Delete**.

   The system prompts for confirmation.

6. Click **OK**.

Manage Roles

Change the Roles Assigned to a User or Group

Use this procedure to assign new roles to a user or group, or to remove existing role assignments.

1. Open the Configuration workspace.
2. Open the User Management page.
3. Open the Users tab.
4. In the **User name or group** field, select the user or group to be changed.
5. Select the roles to be assigned to the user or group, and clear any roles to be removed.
6. Click **Save**.

Create a Custom Role

1. Open the Configuration workspace.
2. Open the User Management page.
3. Open the Roles tab.
4. Click **Add Role** ().

   The Duplicate a User Role dialog opens.
5. In the **Existing user role** field, select the role to be used as a template for the new role.
6. Type a name and description for the role, and then click **OK**.
7. Select the access privileges for the role.
8. Click **Save All Roles**.
9. Click **OK**.

Delete a Custom Role

Note: If a user is assigned only to the role being deleted, then the system prompts for the deletion of the user as well as the role.

1. Open the Configuration workspace.
2. Open the User Management page.
3. Open the Roles tab.
4. Click the **Roles** tab.
5. Click **Delete a Role**.

   The Delete a User Role dialog opens.
6. Select the role to be deleted and then click **OK**.

Export and Import User Management Settings

The SCIEX OS User Management database can be exported and imported. After configuring the User Management database on one SCIEX computer, for example, export it, and then import it on other SCIEX computers, to make sure that the user management settings are consistent.

Only domain users are exported. Local users are not exported.

Before importing user management settings, the software automatically backs up the current settings. The user can restore the last backup.

Export User Management Settings

1. Open the Configuration workspace.
2. Open the User Management page.
3. Click **Advanced > Export User Management settings** .

   The Export User Management Settings dialog opens.
4. Click **Browse**.
5. Browse to and select the folder where the settings will be saved, and then click **Select Folder**.
6. Click **Export**.

   A confirmation message is shown, with the name of the file that contains the exported settings.
7. Click **OK**.

Import User Management Settings

1. Open the Configuration workspace.
2. Open the User Management page.
3. Click **Advanced > Import User Management settings** .

   The Import User Management Settings dialog opens.
4. Click **Browse**.
5. Browse to and select the file that contains the settings to be imported, and then click **Open**.

   The software verifies that the file is valid.
6. Click **Import**.

The software backs up the current user management settings and imports the new settings. A confirmation message is shown.

7. Click **OK**.

Restore User Management Settings

Before importing user management settings, the software backs up the current settings. Use this procedure to restore the last backup of the user management settings.

1. Open the Configuration workspace.
2. Open the User Management page.
3. Click **Advanced > Restore previous settings** .

   The Restore User Management Settings dialog opens.
4. Click **Yes**.
5. Close SCIEX OS and open it again.

Configure Access to Projects and Project Files

Use the Windows security features to control access to the SCIEX OS Data folder. By default, project files are stored in the SCIEX OS Data folder. To access a project, users must have access to the root directory in which the project data is stored. For more information, refer to the section: Windows Security Configuration.

Project Folders

Each project contains folders that store different types of files. For information about the contents of the different folders, refer to the table: Table 4-6.

Table 4-6 Project Folders

Folder	Contents
\Acquisition Methods	Contains the mass spectrometer (MS) and LC methods that have been created within the project. MS methods have the msm extension and LC methods have the lcm extension.
\Audit Data	Contains the project audit map and all of the audit records.
\Batch	Contains all of the acquisition batch files that have been saved. Acquisition batches have the bch extension.

Table 4-6 Project Folders (continued)

Folder	Contents
\Data	Contains the acquisition data files. Acquisition data files have the wiff and wiff2 extensions.
\Project Information	Contains the project default settings files.
\Quantitation Methods	Contains all of the processing method files. Processing methods have the qmethod extension.
\Quantitation Results	Contains all of the quantitation Results Table files. Results Table files have the qsession extension.

Software File Types

For common SCIEX OS file types, refer to the table: Table 4-7.

Table 4-7 SCIEX OS Files

Extension	File Type	Folder
atds	• Workstation audit trail data and archives • Workstation audit trail settings • Project audit trail data and archives • Project audit trail settings	• For projects: <project name>\Audit Data • For the workstation: C:\ProgramData\SCIEX\Audit Data
atms	Audit maps	• For projects: <project name>\Audit Data • For the workstation: C:\ProgramData\SCIEX\Audit Data
bch	Batch	Batch
cset	Results Table settings	Project Information
dad	Mass spectrometry data file	• Optimization • Data
exml	Project default settings	Project Information
journal	Temporary files created by SCIEX OS	Various folders
lcm	LC Method	Acquisition Methods

Table 4-7 SCIEX OS Files (continued)

Extension	File Type	Folder
msm	MS Method	Acquisition Methods
pdf	Portable document data	—
qlayout	Workspace layout	— **Note:** The default workspace layout for a project is stored in the Project Information folder.
qmethod	Processing method	Quantitation Methods
qsession	Results Table **Note:** SCIEX OS can only open qsession files that were created with SCIEX OS.	Quantitation Results
wiff	Mass spectrometry data file compatible with the SCIEX OS software **Note:** SCIEX OS generates both wiff and wiff2 files.	Data
wiff.scan	Mass spectrometry data file	• Optimization • Data
wiff2	Mass spectrometry data file generated by SCIEX OS	• Optimization • Data
xls or xlsx	Excel spreadsheet	Batch
xps	Recalibration	Data\Cal

Network Acquisition 5

This section describes how network acquisition works in SCIEX OS and the benefits and limitations of network-based projects. It also contains procedures for configuring network acquisition.

About Network Acquisition

Network acquisition can be used to acquire data from one or more instruments to network-based project folders that can be processed on remote workstations. This process is network-failure tolerant and makes sure that no data is lost if the network connection fails during acquisition.

System performance can be slower when network projects are being used than it is when local projects are being used. Because some audit trails also reside in the network folders, any activity that generates a project audit record is also slower. Network files might take some time to open, depending on the network performance. Network performance is related not only to the physical network hardware, but also to network traffic and design.

Note: If the ClearCore2 service is interrupted during network acquisition, then the partial sample data for the sample under acquisition at the time of the interruption will not be written to the data file.

Note: When using network acquisition in a regulated environment, synchronize the local computer time with the server time for accurate timestamps. The server time is used for the file creation time. The Audit Trail Manager records the file creation time using the local computer time.

CAUTION: Potential Data Loss. Do not save data from multiple acquisition computers in the same network data file.

Benefits of Using Network Acquisition

Network data acquisition provides a secure method of working with project folders that reside entirely on network servers. This reduces the complexity involved in collecting data locally and then moving the data to a network location for storage. Also, because network drives are typically backed up automatically, the need to back up local drives is reduced or eliminated.

Secure Network Account

In a regulated environment where data is being acquired to a network folder, it is highly recommended that users not have delete rights for the destination folder. However, without delete access to this folder, SCIEX OS cannot perform optimally. The secure network account (SNA) feature identifies a network account that has the Full control file permission for the network root directory. The ClearCore2 service uses this account to transfer data to the network folder.

The SNA must have Full control for:

- The network root directory folder
- The SCIEX OS Data\NetworkBackup folder on the acquisition computer
- The SCIEX OS Data\TempData folder on the acquisition computer

The SNA does not need to:

- Belong to the Administrator group on the computer.
- Be in the SCIEX OS User Management database.

The SNA is specified on the Projects page in the Configuration workspace. Only a valid Windows network or domain account can be specified.

If an SNA is not specified, then SCIEX OS uses the credentials of the currently logged on user to transfer the data to the network root directory. For the transfer to be successful, the account must have write permissions to all project folders to which data is being acquired, regardless of which user submitted the batch for acquisition.

Data Transfer Process

When SCIEX OS acquires data to a network location, it first writes each sample to a folder on the local drive, and then transfers it to the network. When the successful transfer of the entire data file is confirmed, the local folder containing the data is deleted. If the network becomes unavailable during this process, then SCIEX OS tries again every 15 minutes until the transfer is successful.

For information about data access during extended periods of network connectivity loss, refer to the section: Remove Samples from the Network Transfer Folders.

Configure Network Acquisition

A root directory is the folder in which SCIEX OS stores data. To be certain that project information is stored safely, create the root directory using SCIEX OS. Do not create projects in File Explorer.

Optionally, when creating root directories on a network resource, define the **Credentials for Secure Network Account**. This is the secure network account defined on the network resource. Refer to the section: Secure Network Account.

For information about creating projects and subprojects, refer to the document: *SCIEX OS Software User Guide*.

Specify a Secure Network Account

If projects are stored on a network resource, then an SNA can be specified, to make sure that all users of the workstation have the required access to the network resource.

1. Open the Configuration workspace.
2. Click **Projects**.
3. In the **Advanced** section, click **Credentials for Secure Network Account**.
4. Type the user name, password, and domain of the secure network account defined on the network resource.
5. Click **OK**.

Auditing 6

This section explains how to use the auditing functionality. For information about Windows auditing functions, refer to the section: System Audits.

Audit Trails

SCIEX OS organizes audited events by workstation and project in audit trails, which are files that store records of the audited events. Processing audit trail events are contained in the project audit trail map and they are stored with the Results Table. Audit trails, combined with files such as wiff2 files and Results Table files, constitute valid electronic records that can be used for compliance purposes.

Table 6-1 SCIEX OS Audit Trails

Audit Trail	Examples of Events Recorded	Available Audit Maps Stored In	Default Audit Maps

Workstation	• Changes to:
	  • Active audit map assignment
	  • Instrument tuning
	  • Sample queues
	  • Security
	  • Tuning
	  • Devices
		• C:\ProgramData\SCIEX\Audit Data folder	• Silent Audit Map

Project (one per project)	• Changes to:
	  • Active audit map assignment
	  • Project
	  • Data
	• Printing
		• <project>\Audit Data folder	• Specified on the Audit Maps page of the Configuration workspace

After the workstation audit trail or a project audit trail contains 20 000 audit records, SCIEX OS automatically archives the records and begins a new audit trail. For more information, refer to the section: Audit Trail Records.

Audit Maps

Audit maps are files that specify:

- Events that are audited.
- Audited events that require the operator to specify reasons for the change.
- Audited events that require electronic signatures.

The user can create many workstation and project audit maps, but only one audit map can be in use at any given time for each workstation and each project. The audit map in use for a workstation or project is called the active audit map.

Each audit map contains a list of all of the events that can be audited. Depending on where the map is used, the events apply to the workstation audit trail or the project audit trail. For each event, specify whether it is audited, if an electronic signature is required, and up to ten predefined reasons for the event.

When SCIEX OS is installed, the Silent audit map is set as the active audit map that will be used as the default for all new projects on the Audit Maps page in the Configuration workspace. The user can identify a different active audit map to be used as the default for all new projects. Refer to the section: Change the Active Audit Map for a Project.

Setup of Audit Maps

Before working with projects that require auditing, configure audit maps that are appropriate to standard operating procedures. Several default audit map templates are available when SCIEX OS is installed, but it might be necessary to create a customized map. Make sure that one appropriate audit map is available for the workstation audit trail and that one appropriate audit map is available for each project.

Table 6-2 Checklist for Configuring Auditing

Task	Refer To
Create an audit map for the workstation audit trail.	• Create a Workstation Audit Map. • Edit a Workstation Audit Map.
Apply the audit map to the workstation audit trail.	• Change the Active Audit Map for a Workstation.
Create a default active audit map for new projects.	• Create a Project Audit Map.
Configure the audit map to be used for each existing project.	• Create a Project Audit Map. • Edit a Project Audit Map.
Apply an audit map to each existing project.	• Change the Active Audit Map for a Project.

Installed Audit Map Templates

The software includes several audit map templates. These templates cannot be edited or deleted.

Table 6-3 Installed Audit Maps

Audit Map	Description
Example Audit Map	Selected events are audited. For illustration purposes only.
Full Audit Map	All of the events are audited. Electronic signatures and reasons are required for all of the events.
No Audit Map	No events are audited. **Note:** The **Change Active Audit Map Assignment** event is always recorded, even if the No Audit Map template is used.
Silent Audit Map	All of the events are audited. Electronic signatures and reasons are not required for any events.

For descriptions of the types of audit trails and their relationships to audit maps, refer to the table: Table 6-1. For information about the events recorded in audit trails, refer to the section: Audit Trail Records.

For information about the auditing process, refer to the table: Table 6-2.

Work with Audit Maps

SCIEX OS includes several installed audit map templates. For descriptions of the audit map templates, refer to the section: Installed Audit Map Templates. For a checklist of suggested steps for setting up auditing, refer to the section: Setup of Audit Maps.

If an active audit map template is deleted in SCIEX OS or in File Explorer, then the project that uses that audit map template uses the Silent Audit Map.

Project Audit Maps

Project audit maps control the auditing of project events. For a list of auditable project events, refer to the section: Project Audit Trail.

Create a Project Audit Map

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Projects Templates** tab.
4. In the **Edit map template** field, select a template to be used as the basis of the new map.
5. Click **Add Template** ( ).

   The Add a Project Audit Map Template dialog opens.
6. Type the name of the new map, and then click **OK**.
7. Select and configure the events to be recorded by following these steps:
   a. Select the **Audited** check box for the event.
   b. (Optional) If a reason is required, then select **Reason Required**.
   c. (Optional) If an electronic signature is required, then select **E-Sig Required**.
   d. (Optional) If predefined reasons are required, then select **Use Predefined Reason Only** and define the reasons.
8. Make sure that the **Audited** check box is cleared for any events that will not be audited.
9. Click **Save Template**.

   The system prompts the user to apply the new map to projects.
10. Do one of the following:
    - To apply the new map to projects, click **Yes**, select the projects that will use the new map, and then click **Apply**.

- If the new map is not to be applied to existing projects, then click **No**.

11. (Optional) To use this audit map as the default for all new projects, click **Use as Default for New Projects**.

Edit a Project Audit Map

Note: Installed audit map templates cannot be edited.

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Projects Templates** tab.
4. In the **Edit map template** field, select the map to be modified.
5. Select and configure the events to be recorded by following these steps:
   a. Select the **Audited** check box for the event.
   b. (Optional) If a reason is required, then select **Reason Required**.
   c. (Optional) If an electronic signature is required, then select **E-Sig Required**.
   d. (Optional) If predefined reasons are required, then select **Use Predefined Reason Only** and define the reasons.
6. Make sure that the **Audited** check box is cleared for any events that will not be audited.
7. Click **Save Template**.

   The system prompts the user to apply the new map to projects.
8. Do one of the following:
   - To apply the new map to projects, click **Yes**, select the projects that will use the new map, and then click **Apply**.
   - If the new map is not to be applied to existing projects, then click **No**.

Change the Active Audit Map for a Project

When an audit map is applied to the project, it becomes the active audit map. The audit configuration in the active audit map determines which events are recorded in the audit trails.

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Projects Templates** tab.
4. In the **Edit map template** field, select the audit map to be assigned to the project.
5. Click **Apply to Existing Projects**.

The Apply Project Audit Map Template dialog opens.

6. Select the check boxes for the projects to which this audit map will apply.
7. Click **Apply**.

Delete a Project Audit Map

Note: Installed audit map templates cannot be deleted.

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Projects Templates** tab.
4. In the **Edit map template** field, select the map to be deleted.
5. Click **Delete Template**.

   The system prompts for confirmation.
6. Click **Yes**.

Workstation Audit Maps

Workstation audit maps control the auditing of workstation events. For a list of auditable workstation events, refer to the section: Workstation Audit Trail.

Create a Workstation Audit Map

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Workstation Templates** tab.
4. In the **Edit map template** field, select a template to be used as the basis of the new map.
5. Click **Add Template** ( ).

   The Add a Workstation Audit Map Template dialog opens.
6. Type the name of the new map, and then click **OK**.
7. Select and configure the events to be recorded by following these steps:
   a. Select the **Audited** check box for the event.
   b. (Optional) If a reason is required, then select **Reason Required**.
   c. (Optional) If an electronic signature is required, then select **E-Sig Required**.

d. (Optional) If predefined reasons are required, then select **Use Predefined Reason Only** and define the reasons.

8. Make sure that the **Audited** check box is cleared for any events that will not be audited.
9. Click **Save Template**.
10. (Optional) To use this audit map as the active audit map for the workstation, click **Apply to the Workstation**.

Edit a Workstation Audit Map

Note: Installed audit map templates cannot be edited.

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Workstation Templates** tab.
4. In the **Edit map template** field, select the map to be modified.
5. Select and configure the events to be recorded by following these steps:
   a. Select the **Audited** check box for the event.
   b. (Optional) If a reason is required, then select **Reason Required**.
   c. (Optional) If an electronic signature is required, then select **E-Sig Required**.
   d. (Optional) If predefined reasons are required, then select **Use Predefined Reason Only** and define the reasons.
6. Make sure that the **Audited** check box is cleared for any events that will not be audited.
7. Click **Save Template**.
8. (Optional) To use this audit map as the active map for the workstation, click **Apply to the Workstation**.

Change the Active Audit Map for a Workstation

When an audit map is applied to the workstation, it becomes the active audit map. The audit configuration in the active audit map determines which events are recorded in the audit trails.

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Workstation Templates** tab.
4. In the **Edit map template** field, select the map to be applied to the workstation.
5. Click **Apply to the Workstation**.

Delete a Workstation Audit Map

Note: Installed audit map templates cannot be deleted.

1. Open the Configuration workspace.
2. Click **Audit Maps**.
3. Click the **Workstation Templates** tab.
4. In the **Edit map template** field, select the map to be deleted.
5. Click **Delete Template**.

   The system prompts for confirmation.
6. Click **Yes**.

View, Search, Export, and Print Audit Trails

This section provides information about viewing audit trails and archived audit trails. It also provides instructions for exporting, printing, searching, and sorting audit records within audit trails.

View an Audit Trail

1. Open the Audit Trail workspace.
2. Select the audit trail to be viewed:
   - To view the workstation audit trail, click **Workstation**.
   - To view a project audit trail, select the project.
3. To view details for an audit record, select the record.

Search or Filter Audit Records

1. Open the Audit Trail workspace.
2. Select the audit trail to be searched.
3. To search for specific audit record, type text in the **Find in Page** field.

   All occurrences of the specified text on the page are highlighted.
4. To filter the audit trail records, follow these steps:

   a. Click the filter (funnel) icon.

      The Filter Audit Trail dialog opens.

b. Type the filter criteria.

c. Click **OK**.

View an Archived Audit Trail

After an audit trail contains 20 000 audit records, SCIEX OS automatically archives the records and begins a new audit trail. The archived audit trail files are named with the type of audit trail and the date and time. For example, the file name for a workstation audit trail archive has the format WorkstationAuditTrailData-<workstation name>-<YYYY><MMDDHHMMSS>.atds

This procedure can also be used to open an audit trail for a Results Table.

1. Open the Audit Trail workspace.
2. Click **Browse**.
3. Browse to and select the archived audit trail to be opened, and then click **OK**.

Note: To open the audit trail for a Results Table, select the associated qsession file.

Print an Audit Trail

1. Open the Audit Trail workspace.
2. Select the audit trail to be printed.
3. Click **Print**.

   The Print dialog opens.
4. Select the printer and then click **OK**.

Export Audit Trail Records

1. Open the Audit Trail workspace.
2. Select the audit trail to be exported.
3. Click **Export**.
4. Browse to the location in which the exported file will be stored, type a **File name**, and then click **Save**.

   The audit trail is saved as a comma-separated value (csv) file.

Audit Trail Records

This section provides more information about audit trails and audit maps. For lists of all of the events that are recorded in the workstation and project audit trails, refer to the sections: Workstation Audit Trail and Project Audit Trail.

The workstation and project audit trails are encrypted files.

Note: Workstation audit trails and archives are stored in the Program Data\SCIEX\Audit Data folder. Project audit trails and archives are stored in the Audit Data folder for the project.

Table 6-4 Event Record Fields

Field	Description
Timestamp	Date and time of the record.
Event Name	The module that generated the event.
Description	A description of the event.
Reason	Reason for the change, as specified by the user, if required.
E-signature	Whether an electronic signature was provided.
Full User Name	The name of the user.
User	The user principal name (UPN) of the user.
Category	The type of event.

Audit Trail Archives

Audit records accumulate in the project audit trail and workstation audit trail and can create large files that are difficult to navigate and manage.

When an audit trail reaches 20,000 records, it is archived. A final archive record is added to the audit trail, and then the audit trail is saved with a name indicating the type of audit trail and the date and time. A new audit trail is created. The first record in the new audit trail states that the audit trail has been archived, and specifies the path to the archived audit trail.

Workstation audit trail archives are stored in the C:\ProgramData\SCIEX\Audit Data folder. The file names are in the format WorkstationAuditTrailData-<workstation name>-<YYYY><MMDDHHMMSS>.atds. For example, WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds.

Project audit trail archives are stored in the Audit Data folder for the project.

Access Data During Network Disruptions

A

View and Process Data Locally

If a temporary network disruption occurs during network acquisition, then the acquired data can be accessed from the NetworkBackup folder on the acquisition computer. To avoid corruption of the data, we recommend that the data files in the NetworkBackup folder be copied to a new location before being viewed or processed, and that the original copy of the files be kept in the NetworkBackup folder.

Every 15 minutes, SCIEX OS determines whether the network location is available. If it is, then the transfer of data resumes.

The NetworkBackup folder is stored in the local root directory, typically D:\SCIEX OS Data\NetworkBackup. The data files for each batch are stored in a folder with a unique identifier as the folder name. The date and time stamps of the folders show the batch start date and time, and they can be used to determine which folder contains the data of interest.

Remove Samples from the Network Transfer Folders

If network connectivity is lost for an extended period, or if the network root directory is changed, then it might be necessary to remove data files from the network transfer folders. We recommend that this action be performed by a system administrator with a high level of network technical skill.

1. Open the Queue workspace.
2. Stop the Queue.
3. Cancel all of the remaining samples in the batch that contains the samples to be removed.
4. Close SCIEX OS.
5. Stop **Clearcore2.Service.exe**.

Tip! Perform this task from the Windows Services Manager.

6. Move all files and folders in the OutBox and NetworkBackup folders that are waiting for transfer to the unavailable root directory to another folder temporarily. Do not delete the OutBox or NetworkBackup folders.

   Note: The OutBox folder is a hidden folder in the local root directory, typically D:\SCIEX OS Data\TempData\Outbox. When the files and folders in the Outbox are no longer needed, they can be removed.

   CAUTION: Potential Data Loss. Do not delete the file if the data in the stuck sample must be preserved.

7. Start SCIEX OS.

   Within 15 minutes, SCIEX OS attempts to connect to the network resource. If the connection is successful, then the transfer resumes. When the transfer is complete, the folders in the NetworkBackup folder are deleted.

Audit Events B

This section lists the audit events in SCIEX OS. It also lists the corresponding audit events in the Analyst software, for users who are migrating from the Analyst software to SCIEX OS.

Project Audit Trail

Each project has a project audit trail. The Project Audit Trail is stored in the Audit Data folder for the project. The audit trail file name is ProjectAuditEvents.atds.

Table B-1 Project Audit Trail Events

SCIEX OS	Analyst Software
Explorer Workspace	
Open Sample(s)	Project Events: Data File has been opened
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
Analytics Workspace	
File saved	Project Events: Quantitation Results Table has been created, Quantitation Results Table has been modified, Quantitation Events: Results Table has been saved
Sample Name changed	Quantitation Events: 'Sample Name' has been changed
Sample ID changed	Quantitation Events: 'Sample ID' has been changed
Dilution Factor changed	Quantitation Events: 'Dilution Factor' has been changed
Sample Type changed	Quantitation Events: 'Sample Type' has been changed
Actual Concentration changed	Quanitation Events: 'Concentration' has been changed
Barcode ID changed	—

Table B-1 Project Audit Trail Events (continued)

SCIEX OS	Analyst Software
Used column selection changed	Quantitation Events: 'Use It' has been changed
Samples added or removed	Quantitation Events: Files have been added to Results Table, Files have been removed from Results Table, Samples have been added/removed
Integration cleared	—
External calibration changed	—
External calibration exported	—
Integration parameters changed	Quantitation Events: Quantitation peak has been integrated
Manual Integration	Quantitation Events: Quantitation Peak has been integrated
Results Table created	Quantitation Events: Results table has been created
Processing method changed and applied	Quantitation Events: Quantitation method has been changed
Custom columns modified	Quantitation Events: 'Custom Title' has changed
Data transferred to LIMS	—
Results Table locked	—
Results Table unlocked	—
Results Table approved	Quantitation Events: QA reviewer has accessed a results table
Report created	Project Events: Printing document on printer, Finished printing document on printer
Library search result changed	—
Data exported	—
Window/pane printed	Project Events: Printing document on printer, Finished printing document on printer
Data exploration opened	Project Events: Data File has been opened

Table B-1 Project Audit Trail Events (continued)

SCIEX OS	Analyst Software
Formula column changed	Quantitation Events: Formula name has been changed, Formula name has been added, Formula string has been changed, Formula column has been removed
Comparison sample changed in non-targeted workflow	—
MS/MS selection changed	—
Std. Addition Actual concentration changed	—
Manual Integration reverted	Quantitation Events: Quantitation peak has been reverted back to original
Auto-Processing File saved	—
Audit Map Page	
Project Audit Map changed	Project Events: Project Settings have been changed
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Batch Workspace	
Batch information imported from LIMS/text	—
Print	Project Events: Printing Document on printer, Finished printing document on printer
MS Method Workspace	
Print	Project Events: Printing Document on printer, Finished printing document on printer
LC Method Workspace	
Print	Project Events: Printing Document on printer, Finished printing document on printer
Queue Workspace	
Sample Transferred	—

Workstation Audit Trail

Each workstation has one workstation audit trail. The workstation audit trail is stored in the Program Data\SCIEX\Audit Data folder. The audit trail file name is in the format: WorkstationAuditTrailData.atds.

Table B-2 Workstation Audit Trail Events

SCIEX OS	Analyst Software
Instrument Tune	
Firmware changed	—
Manual Tuning	Instrument Events: Tune parameter settings changed
Automatic Tuning	Instrument Events: Tune parameter settings changed
Print Procedure Result in MS Tune	Project Events: Printing Document on printer, Finished printing document on printer
Hardware Configuration	
Devices Activated	Instrument Events: Hardware profile has been activated
Devices Deactivated	Instrument Events: Hardware profile has been deactivated
UserLog	
Print Event Log	—
Data File Checksum	
Wiff data file checksum has been changed	—
Security	
User added/deleted	Instrument Events: User Added, User Deleted
User role assigned to user/user group	Instrument Events: User Changed User Type
User role modified	Instrument Events: User Type Changed
User has logged in	Instrument Events: User Logged In
User has logged out	Instrument Events: User Logged out
User Login Failed	Instrument Events: User Login Failed

Table B-2 Workstation Audit Trail Events (continued)

SCIEX OS	Analyst Software
User role deleted	Instrument Events: User Type Deleted
Secure Network Account credentials have been specified	Instrument Events: Acquisition Account Changed
Secure Network Account credentials have been removed	Instrument Events: Acquisition Account Changed
Secure Network Account credentials have been changed	Instrument Events: Acquisition Account Changed
User has turned off exclusive mode	—
Security configuration changed	Instrument Events: The Security Configuration has been modified, Screen Lock Changed, Auto Logout changed
Auto logoff by system	Instrument Events: User Logged out
Forced logoff by another user	Instrument Events: User Logged out
Screen unlock failed	—
Forced Logoff failed	—
User management settings have been imported	—
User management settings have been exported	—
User management settings have been restored	—
Explorer Workspace	
Open Sample(s)	Project Events: Data File has been opened
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Audit Map Page	
Workstation Audit Map changed	Instrument Events: Instrument Settings have been changed
Workstation Audit Trail printed	—
Workstation Audit Trail exported	—

Table B-2 Workstation Audit Trail Events (continued)

SCIEX OS	Analyst Software
Queue Workspace	
Sample moved in Queue	Instrument Events: Sample moved from position x to position y of Batch File
Batch moved in Queue	Instrument Events: Move Batch
Reaquiring sample	Instrument Events: Reacquiring sample(s)
Sample starts to acquire	—
Print Queue	Project Events: Printing Document on printer, Finished printing document on printer
Sample acquistion has completed	Project Events: Sample has been added to Data file
Automatic reinjections Occurred	—
Automatic injection Occurred	—

Mapping of Permissions Between SCIEX OS and the Analyst Software

C

This section is provided for users who are migrating from the Analyst software to SCIEX OS, to help them migrate their user security settings. It shows the Analyst software permissions that correspond to SCIEX OS permissions.

Table C-1 Permission Mapping

SCIEX OS	Analyst Software
Batch Workspace	
Submit unlocked methods	—
Open	Batch: Open Existing Batches
Save as	Batch: Create New Batches, Import, Edit Batches, Save Batches, Overwrite Batches
Submit	Batch: Submit Batches
Save	Batch: Save Batches, Overwrite Batches
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Configuration Workspace	
General tab	—
General: change regional setting	—
General: full screen mode	—
LIMS Communication tab	—
Audit maps tab	Audit Trail Manager: Change Audit Trail Settings, Create or Modify Audit Maps
Queue tab	—
Queue: instrument idle time	—
Queue: max. number of acquired samples	—

Table C-1 Permission Mapping (continued)

SCIEX OS	Analyst Software
Queue: other queue settings	—
Projects tab	—
Projects: create project	Analyst Application: Create Project
Projects: apply an audit map template to an existing project	Audit Trail Manager: Change Audit Trail Settings
Projects: create root directory	Analyst Application: Create Root Directory
Project: set current root directory	Analyst Application: Set Root Directory
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	Hardware Configuration: Create, Delete, Edit, Activate/Deactivate
User management tab	Security Config
Force user logoff	Unlock/Logout Application
Event Log Workspace	
Access event log workspace	—
Archive log	—
Audit Trail Workspace	
Access audit trail workspace	Audit Trail Manager: View Audit Trail Data
View active audit map	Audit Trail Manager: View Audit Trail Data
Print/Export audit trail	Audit Trail Manager: View Audit Trail Data
Data Acquisition Panel	
Start	—
Stop	—
Save	—
MS Method and LC Method Workspaces	
Access method workspace	—

Table C-1 Permission Mapping (continued)

SCIEX OS	Analyst Software
New	Acquisition Method: Create/Save acquisition method
Open	Acquisition Method:Open acquisition method as read-only (acquire mode)
Save	Acquisition Method: Overwrite acquisition methods, Create/Save acquisition method
Save as	Acquisition Method: Overwrite acquisition methods, Create/Save acquisition method
Lock/Unlock method	—
Queue Workspace	
Manage	Sample Queue: Reacquire, Delete Sample or Batch, Move Batch
Start/Stop	Sample Queue: Start Sample, Stop Sample, Abort Sample, Stop Queue
Print	Report Template Editor: Print
Library Workspace	
Access library workspace	Explore: Setup library location, Setup library user options, Add library record, Add spectrum to library, Modify library record (overrides add/delete if disabled), Delete MS spectrum, Delete UV spectrum, Delete structure, View library, Search library
MS Tune Workspace	
Access MS Tune workspace	—
Advanced MS tuning	Tune: Instrument Optimization, Manual Tune, Edit Tuning Options
Advanced troubleshooting	—
Quick status check	Tune: Insturment Opt
Restore instrument data	Tune: Edit Tuning Options, Edit instrument data
Explorer Workspace	
Access explorer workspace	—

Table C-1 Permission Mapping (continued)

SCIEX OS	Analyst Software
Export	Explore: Save data to text file
Print	Report Template Editor: Print
Options	—
Recalibrate	Tune: Calibrate from current spectrum
Analytics Workspace	
New results	Quantitation: Create new results tables
Create processing method	Quantitation: Create quantitation methods
Modify processing method	Quantitation: Modify existing methods
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	Quantitation: Change default method options
Change default quantitation method integration parameters	Quantitation: Change default method options
Enable project modified peak warning	—
Project secure export settings	—
Add samples	Quantitation: Add and Remove samples from results table
Remove selected samples	Quantitation: Add and Remove samples from results table
Export, import or remove external calibration	—
Modify sample name	Quantitation: Modify sample name
Modify sample type	Quantitation: Modify Sample Type
Modify sample ID	Quantitation: Modify Sample ID
Modify actual concentration	Quantitation: Modify Analyte Concentration
Modify dilution factor	Quantitation: Modify Dilution Factor
Modify comments fields	Quantitation: Modify Sample Comment
Enable manual integration	Quantitation: Manually integrate

Table C-1 Permission Mapping (continued)

SCIEX OS	Analyst Software
Set peak to not found	—
Include or exclude a peak from the results table	Quantitation: Exclude standards from calibration
Regression options	Quantitation: Change regression parameters
Modify the results table integration parameters for a single chromatogram	Quantitation: Change "simple" parameters in peak review, Change "advanced" parameters in peak review
Modify quantitation method for results table component	Quantitation: Edit results tables' method
Create metric plot new settings	Quantitation: Modify or create metric plot settings
Add custom columns	Quantitation: Create or modify formula columns
Set peak review title format	—
Remove custom column	Quantitation: Create or modify formula columns
Results table display settings	Quantitation: Change results table column precision, Change results table column visibility, Modify results table settings
Lock results table	—
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	Report Template Editor: Create/Modify report templates
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—
Add the MSMS spectra to library	Explore: Add spectrum to library record
Project default settings	Quantitation: Modify global (default) settings
Create report in all formats	—
Edit flagging criteria parameters	—
Automatic outlier removal parameter change	—

Table C-1 Permission Mapping (continued)

SCIEX OS	Analyst Software
Enable automatic outlier removal	—
Update processing method via FF/LS	—
Update results via FF/LS	—
Enable grouping by adducts functionality	Quantitation: Create Analyte Groups, Modify Analyte Groups
Browse for files	—
Enable standard addition	—
Set Manual Integration Percentage Rule	Quantitation: Enable or Disable percent rule in Manual Integration

Data File Checksum D

We recommend that users use datafile checksums for wiff files. The checksum feature is a cyclic redundancy check to verify data file integrity.

If the Data File Checksum feature is enabled, then whenever the user creates a data (wiff) file, the software generates a checksum value using an algorithm based on the MD5 public encryption algorithm and saves the value in the file. When the checksum is verified, the software calculates the checksum and compares the calculated checksum to the checksum stored in the file.

The checksum comparison can have three outcomes:

- If the values match, then the checksum is valid.
- If the values do not match, then the checksum is invalid. An invalid checksum indicates that either the file has been modified outside of the software or the file was saved when checksum calculation was enabled and the checksum is different from the original checksum.
- If the file has no stored checksum value, then the checksum is not found. A file has no stored checksum value because the file was saved when the Data File Checksum feature was disabled.

Note: The user can verify the checksum using the Analyst software. Refer to the documentation for the Analyst software.

Enable or Disable the Data File Checksum Feature

1. Open the Configuration workspace.
2. Click **Projects**.
3. If required, expand **Data File Security**.
4. To enable the data file checksum feature, select the **Enable checksum writing for wiff1 data creation** check box. To disable the feature, clear this check box.

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

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 *Customer Reference* DVD that comes with 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.