
SCIEX OS Software

Laboratory Director Guide



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

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

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

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

(GEN-IDV-09-10816-D)

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

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

AB Sciex™ is being used under license.

© 2022 DH Tech. Dev. Pte. Ltd.



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

Contents

| | |
|---|-----------|
| 1 Introduction | 6 |
| 2 Security Configuration Overview | 7 |
| Security and Regulatory Compliance | 7 |
| Security Requirements | 7 |
| SCIEX OS and Windows Security: Working Together | 7 |
| Audit Trails within SCIEX OS and Windows | 8 |
| Customer Security Guidance: Backups | 8 |
| 21 CFR Part 11 | 9 |
| System Configuration | 9 |
| Windows Security Configuration | 9 |
| Users and Groups | 10 |
| Active Directory Support | 10 |
| Windows File System | 10 |
| File and Folder Permissions | 11 |
| System Audits | 11 |
| Event Logs | 11 |
| Windows Alerts | 11 |
| 3 Electronic Licensing | 12 |
| Borrow a Server-based Electronic License | 12 |
| Return a Server-based Electronic License | 13 |
| 4 Access Control | 15 |
| Location of Security Information | 15 |
| Software Security Workflow | 15 |
| Install SCIEX OS | 16 |
| System Requirements | 17 |
| Preset Auditing Options | 17 |
| Configure the Security Mode | 17 |
| Select the Security Mode | 18 |
| Configure Workstation Security Options (Mixed Mode) | 18 |
| Configure E-mail Notification (Mixed Mode) | 19 |
| Configure Access to SCIEX OS | 20 |
| SCIEX OS Permissions | 21 |
| About Users and Roles | 28 |
| Manage Users | 35 |

Contents

| | |
|--|-----------|
| Manage Roles | 36 |
| Export and Import User Management Settings | 37 |
| Export User Management Settings | 37 |
| Import User Management Settings | 38 |
| Restore User Management Settings | 38 |
| Configure Access to Projects and Project Files | 38 |
| Project Folders | 38 |
| Software File Types | 39 |
| 5 Central Administrator Console | 42 |
| Users | 42 |
| User Pool | 42 |
| User Roles and Permissions | 43 |
| Workgroups | 51 |
| Create a Workgroup | 51 |
| Delete a Workgroup | 52 |
| Add Users or Groups to a Workgroup | 52 |
| Add Workstations to a Workgroup | 53 |
| Add Projects to a Workgroup | 54 |
| Manage Projects | 54 |
| About Projects and Root Directories | 54 |
| Add a Root Directory | 55 |
| Delete a Project Root Directory | 55 |
| Add a Project | 56 |
| Add a Subfolder | 56 |
| Workstations | 57 |
| Add a Workstation | 57 |
| Delete a Workstation | 57 |
| Reports and Security Features | 58 |
| Generate Workgroup Data Reports | 58 |
| Export CAC Software Settings | 58 |
| Import CAC Software Settings | 58 |
| Restore CAC Software Settings | 59 |
| 6 Network Acquisition | 60 |
| About Network Acquisition | 60 |
| Benefits of Using Network Acquisition | 60 |
| Secure Network Account | 60 |
| Data Transfer Process | 61 |
| Configure Network Acquisition | 61 |
| Specify a Secure Network Account | 62 |
| 7 Auditing | 63 |
| Audit Trails | 63 |

| | |
|---|-----------|
| Audit Maps | 64 |
| Setup of Audit Maps | 65 |
| Installed Audit Map Templates | 65 |
| Work with Audit Maps | 66 |
| Project Audit Maps | 66 |
| Workstation Audit Maps | 68 |
| View, Search, Export, and Print Audit Trails | 70 |
| View an Audit Trail | 70 |
| Search or Filter Audit Records | 70 |
| View an Archived Audit Trail | 71 |
| Print an Audit Trail | 71 |
| Export Audit Trail Records | 71 |
| Audit Trail Records | 72 |
| Audit Trail Archives | 72 |
| | |
| A Access Data During Network Disruptions | 73 |
| View and Process Data Locally | 73 |
| Remove Samples from the Network Transfer Folders | 73 |
| | |
| B Audit Events | 75 |
| | |
| C Mapping of Permissions Between SCIEX OS and the Analyst Software | 82 |
| | |
| D Data File Checksum | 88 |
| Enable or Disable the Data File Checksum Feature | 88 |
| | |
| Contact Us | 89 |
| Customer Training | 89 |
| Online Learning Center | 89 |
| SCIEX Support | 89 |
| CyberSecurity | 89 |
| Documentation | 89 |

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.

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

Security Configuration Overview

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](#).

Customer Security Guidance: Backups

Backup of customer data is the responsibility of the customer. Although SCIEX service and support personnel might provide advice and recommendations about customer data backup, it is up to the customer to make sure the data is backed up according to the policies, needs, and regulatory requirements of the customer. The frequency and coverage of customer data backup should be commensurate with organizational requirements and the criticality of the data that is generated.

Customers should make sure that backups are functional, because backups are a vital component of overall data management and essential to recovery in the event of a malicious attack, hardware failure, or software failure. Do not back up the computer during data acquisition, or else make sure that files being acquired are ignored by the backup software. We strongly recommend that a full backup be taken of the computer before any security updates are installed or any computer repairs are performed. This will facilitate a rollback in the rare case that a security patch affects any application functionality.

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 Parameters 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 Parameters 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 the previous password.

Security Configuration Overview

- 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 service 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.

For SCIEX OS, electronic licensing can be node-locked or server-based. For the Central Administrator Console (CAC) software, electronic licensing can only be node-locked.

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.

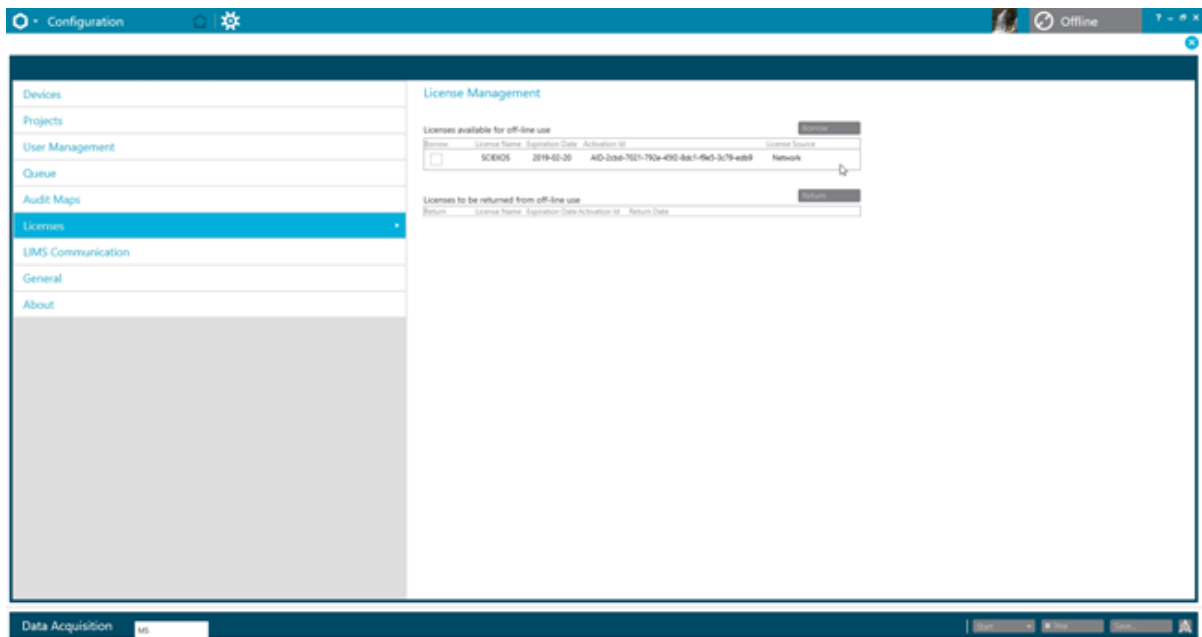
Borrow a Server-based Electronic License

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.

Note: This procedure is not applicable for the Central Administrator Console (CAC) software.

1. Open the Configuration workspace.
2. Click **Licenses**.
The Licenses available for off-line use table shows all of the licenses available for borrowing.

Figure 3-1 License Management: Borrow a License



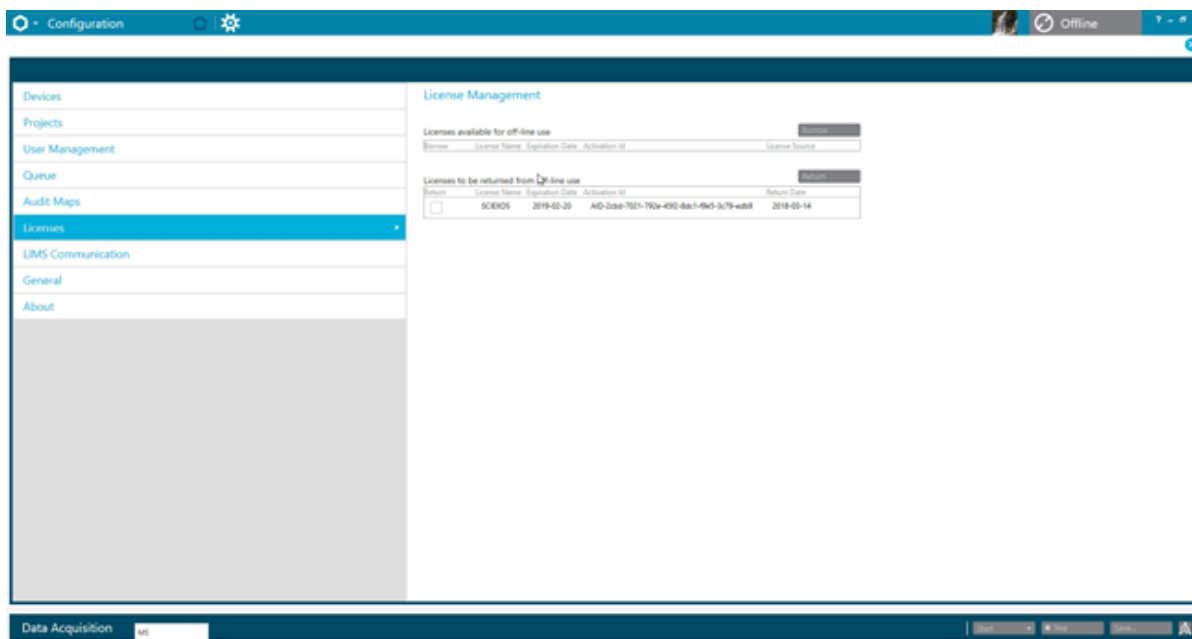
3. Select the license to be borrowed, and then click **Borrow**.

Return a Server-based Electronic License

Note: This procedure is not applicable for the Central Administrator Console (CAC) software.

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**.

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.

This procedure provides instructions for local administration of SCIEX OS. For centralized administration of SCIEX OS, refer to the section: [Central Administrator Console](#)

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](#).

Access Control

Table 4-1 Workflow for Configuring Security

| Task | Procedure |
|---|--|
| Install SCIEX OS. | Refer to the document: <i>SCIEX OS Software Installation Guide</i> . |
| 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 or web download package: *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 the software, then that user has access to SCIEX OS.

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

Mixed Mode: Users log on to Windows and the software separately. The credentials used to log on to Windows need not be the same as the credentials used to log on to . 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 the software 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 the software 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.

Access Control

Note: For workgroups administered by the Central Administrator Console (CAC) software, the security mode cannot be managed with SCIEX OS.

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 |
|---|
| <ul style="list-style-type: none">• 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](#).

The software 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 the software installed 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

The screenshot shows the SCIEX OS User Management page. The left sidebar contains navigation links: Devices, Projects, User Management (selected), Queue, Audit Maps, Licenses, LIMS Communication, General, and About. The main content area is titled 'User Roles and Permission Categories' and displays a table of permissions for four roles: Administrator, Method Developer, Analyst, and Reviewer.

| 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 | | | | |
| General tab | ✓ | ✓ | ☐ | ☐ |
| General: change regional setting | ✓ | ✓ | ☐ | ☐ |
| General: full screen mode | ✓ | ✓ | ☐ | ☐ |
| LIMS communication tab | ✓ | ✓ | ☐ | ☐ |

Table 4-3 Permissions

| Permission | Description |
|---------------------------------|--|
| Batch | |
| Submit unlocked methods | Lets users submit batches that contain unlocked methods. |
| Open | Lets users open existing batches. |
| Save as | Lets users save batches with a new name. |
| Submit | Lets users submit batches. |
| Save | Lets users save a batch, overwriting the existing content. |
| Save ion reference table | Lets users edit the ion reference table. |

Access Control

Table 4-3 Permissions (continued)

| Permission | Description |
|---|---|
| Add data sub-folders | Lets users create subfolders to store data. |
| Configure Decision Rules | Lets users add and change decision rules. |
| Configuration | |
| General tab | Lets users open the General page in the Configuration workspace. |
| General: change regional setting | Lets users apply current system regional settings to SCIEX OS. |
| General: full screen mode | Lets users enable and disable Full Screen mode. |
| General: Stop Windows services | Lets users enable or disable the Windows Settings option. |
| LIMS communication tab | Lets users open the LIMS Communication page in the Configuration workspace. |
| Audit maps tab | Lets users open the Audit Maps page in the Configuration workspace. |
| Queue tab | Lets users open the Queue page in the Configuration workspace. |
| Queue: instrument idle time | Lets users set the instrument idle time. |
| Queue: max number of acquired samples | Lets users set the maximum number of acquired samples allowed. |
| Queue: other queue settings | Lets users configure other queue settings. |
| Projects tab | Lets users open the Projects page in the Configuration workspace. |
| Projects: create project | Lets users create projects. |
| Projects: apply an audit map template to an existing project | Lets users apply an audit map to a project. |
| Projects: create root directory | Lets users create a root directory to store projects. |
| Projects: set current root directory | Lets users change the root directory for a project. |

Table 4-3 Permissions (continued)

| Permission | Description |
|---|--|
| Projects: specify network credentials | Lets users 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 | Lets users configure the software to write checksums to wiff data files. |
| Projects: clear root directory | Lets users delete a root directory from the list. |
| Devices tab | Lets users open the Devices page in the Configuration workspace. |
| User management tab | Lets users open the User Management page in the Configuration workspace. |
| Force user logoff | Lets users force the log off of a user who is currently logged on to SCIEX OS. Lets users force the log off of a user who is currently logged on to the SCIEX OS software. |
| Event Log | |
| Access event log workspace | Lets users open the Event Log workspace. |
| Archive log | Lets users archive the event log. |
| Audit Trail | |
| Access audit trail workspace | Lets users open the Audit Trail workspace. |
| View active audit map | Lets users view the active audit map for a workstation or project in the Audit Trail workspace. |
| Print/Export audit trail | Lets users print or export the audit trail. |
| CAC Server (CAC only) | |
| Manage Workgroups | Lets users create and manage workgroups in User Management workspace. |
| Manage Workgroups Projects | Lets users create and manage workgroup projects in User Management workspace. |
| Data Acquisition Panel | |
| Start | Lets users start acquisition in the Data Acquisition pane. |
| Stop | Lets users stop acquisition in the Data Acquisition pane. |

Access Control

Table 4-3 Permissions (continued)

| Permission | Description |
|-------------------------------|--|
| Save | Lets users save acquired data with a different file name in the Data Acquisition pane. |
| MS & LC Method | |
| Access method workspace | Lets users open the MS Method and LC Method workspaces. |
| New | Lets users create MS and LC methods. |
| Open | Lets users open MS and LC methods. |
| Save | Lets users save a method, overwriting the existing content. |
| Save as | Lets users save methods with a new name. |
| Lock/Unlock method | Lets users lock methods, to prevent editing, and to unlock methods. |
| Queue | |
| Manage | Lets users open the Queue workspace. |
| Start/Stop | Lets users start or stop the queue. |
| Print | Lets users print the queue. |
| Library | |
| Access library workspace | Lets users open the Library workspace. Not applicable to the Quantitation workflow. |
| CAC settings | |
| Enable Central Administration | Lets users configure SCIEX OS for central administration with the Central Administrator Console (CAC) software. |
| MS Tune | |
| Access MS Tune workspace | Lets users open the MS Tune workspace. |
| Advanced MS tuning | (X500 QTOF Systems) Lets users 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 | Lets users open the Advanced Troubleshooting dialog. |
| Quick status check | (X500 QTOF Systems) Lets users perform the Positive and Negative Quick Status Checks. |
| Restore instrument data | Lets users restore previously saved tuning settings. |

Table 4-3 Permissions (continued)

| Permission | Description |
|--|---|
| Explorer | |
| Access Explorer workspace | Lets users open the Explorer workspace. |
| Export | Lets users export data from the Explorer workspace. |
| Print | Lets users print data in the Explorer workspace. |
| Options | Lets users modify the options for the Explorer workspace. |
| Recalibrate | Lets users recalibrate samples and spectra in the Explorer workspace. Not applicable to the Quantitation workflow. |
| Analytics | |
| New results | Lets users create Results Tables. |
| Create processing method | Lets users create processing methods. |
| Modify processing method | Lets users modify processing methods. |
| Allow Export and Create Report of unlocked Results Table | Lets users export or generate a report from a Results Table or statistics table, if the Results Table is not locked. |
| Save results for Automation Batch | Lets Results Tables created automatically in the Batch workspace be saved. This permission is required for autoprocessing during acquisition. |
| Change default quantitation method integration algorithm | Lets users change the integration algorithm in the project default settings. |
| Change default quantitation method integration parameters | Lets users change the integration parameters in the project default settings. |
| Enable project modified peak warning | Lets users enable the modified peak warning property for a project. |
| Add samples | Lets users add samples to a Results Table. |
| Remove selected samples | Lets users remove samples from a Results Table. |
| Export, import, or remove external calibration | Lets users export, import, or remove external calibrations. |
| Modify sample name | Lets users modify the sample name in the Results Table. |
| Modify sample type | Lets users modify the sample type, such as standard, quality control (QC), or unknown, in the Results Table. |

Access Control

Table 4-3 Permissions (continued)

| Permission | Description |
|---|--|
| Modify sample ID | Lets users modify the sample ID in the Results Table. |
| Modify actual concentration | Lets users modify the actual concentration of the standard and QC samples in the Results Table. |
| Modify dilution factor | Lets users modify the dilution factor in the Results Table. |
| Modify comment fields | Lets users modify comment fields: <ul style="list-style-type: none">• Component Comment• IS Comment• IS Peak Comment• Peak Comment• Sample Comment |
| Enable manual integration | Lets users perform manual integration. |
| Set peak to Not Found | Lets users set a peak to Not Found . |
| Include or exclude a peak from the Results Table | Lets users include and exclude peaks from the Results Table. |
| Regression options | Lets users change the regression options in the Calibration Curve pane. |
| Modify Results Table integration parameters for a single chromatogram | Lets users change integration parameters for a single chromatogram in the Peak Review pane. |
| Modify quantitation method for the Results Table component | Lets users 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 | Lets users create new Metric Plots and change the settings. |
| Add custom columns | Lets users add custom columns to a Results Table. |
| Set peak review title format | Lets users change the peak review title. |
| Remove custom column | Lets users remove custom columns from a Results Table. |
| Results Table display settings | Lets users customize the columns shown in the Results Table. |
| Lock Results Table | Lets users lock a Results Table to prevent editing. |

Table 4-3 Permissions (continued)

| Permission | Description |
|---|--|
| Unlock Results Table | Lets users unlock a Results Table to allow editing. |
| Mark Results file as reviewed and save | Lets users mark a Results Table as reviewed and save it. |
| Modify report template | Lets users change report templates. |
| Transfer results to LIMS | Lets users upload results to a Laboratory Information Management System (LIMS). |
| Modify barcode column | Lets users change the Barcode column in a Results Table. |
| Change comparison sample assignment | Lets users change the comparison sample specified in the Comparison column of the Results Table. |
| Add the MSMS spectra to library | Lets users add the selected MS/MS spectra to a library. Not applicable to the Quantitation workflow. |
| Project default settings | Lets users change the project default quantitative and qualitative processing settings. |
| Create report in all formats | Lets users generate reports in all formats. Users without this permission can only generate reports in PDF format. |
| Edit flagging criteria parameters | Lets users change the flagging parameters in a processing method. |
| Automatic outlier removal parameter change | Lets users change the parameters for automatic outlier removal. |
| Enable automatic outlier removal | Lets users change the processing method to turn on the automatic outlier removal feature. |
| Update processing method via FF/LS | Lets users update processing methods using Formula Finder and Library Search. Not applicable to the Quantitation workflow. |
| Update results via FF/LS | Lets users update the results using Formula Finder and Library Search. Not applicable to the Quantitation workflow. |
| Enable grouping by adducts functionality | Lets users update the processing method to turn on the grouping adducts feature. |
| Browse for files | Lets users browse outside of the local data folder. |
| Enable standard addition | Lets users update the processing method to turn on the standard addition feature. |

Access Control

Table 4-3 Permissions (continued)

| Permission | Description |
|---|--|
| Set Manual Integration Percentage Rule | Lets users 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.

Note: For workgroups administered by the Central Administrator Console (CAC) software, the User Management pages are read-only.

Table 4-4 Predefined Roles

| Role | Typical Tasks |
|-------------------------|---|
| Administrator | <ul style="list-style-type: none">• Manages the system.• Configures security. |
| Method Developer | <ul style="list-style-type: none">• Creates methods.• Runs batches.• Analyzes data for use by the end-user. |
| Analyst | <ul style="list-style-type: none">• Runs batches.• Analyzes data for use by the end-user. |
| Reviewer | <ul style="list-style-type: none">• Reviews data.• Reviews audit trails.• Reviews quantitation results. |

Table 4-5 Preset Permissions

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|--------------|---------------|------------------|---------|----------|
| Batch | | | | |

Table 4-5 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|---------------------------------------|---------------|------------------|---------|----------|
| Submit unlocked methods | ✓ | ✓ | ✓ | × |
| Open | ✓ | ✓ | ✓ | ✓ |
| Save as | ✓ | ✓ | ✓ | × |
| Submit | ✓ | ✓ | ✓ | × |
| Save | ✓ | ✓ | ✓ | × |
| Save ion reference table | ✓ | ✓ | ✓ | × |
| Add data sub-folders | ✓ | ✓ | ✓ | × |
| Configure Decision Rules | ✓ | ✓ | ✓ | × |
| Configuration | | | | |
| General tab | ✓ | ✓ | × | × |
| General: change regional setting | ✓ | ✓ | × | × |
| General: full screen mode | ✓ | ✓ | × | × |
| General: Stop Windows services | ✓ | × | × | × |
| LIMS communication tab | ✓ | ✓ | × | × |
| Audit maps tab | ✓ | × | × | × |
| Queue tab | ✓ | ✓ | ✓ | ✓ |
| Queue: instrument idle time | ✓ | ✓ | × | × |
| Queue: max number of acquired samples | ✓ | ✓ | × | × |
| Queue: other queue settings | ✓ | ✓ | × | × |
| Projects tab | ✓ | ✓ | ✓ | ✓ |

Access Control

Table 4-5 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|--|---------------|------------------|---------|----------|
| 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 | ✓ | × | × | × |
| 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 | ✓ | ✓ | ✓ | × |

Table 4-5 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|-------------------------------|---------------|------------------|---------|----------|
| Stop | ✓ | ✓ | ✓ | × |
| Save | ✓ | ✓ | ✓ | × |
| MS & LC Method | | | | |
| Access method workspace | ✓ | ✓ | ✓ | ✓ |
| New | ✓ | ✓ | × | × |
| Open | ✓ | ✓ | ✓ | ✓ |
| Save | ✓ | ✓ | × | × |
| Save as | ✓ | ✓ | × | × |
| Lock/Unlock method | ✓ | ✓ | × | × |
| Queue | | | | |
| Manage | ✓ | ✓ | ✓ | × |
| Start/Stop | ✓ | ✓ | ✓ | × |
| Print | ✓ | ✓ | ✓ | ✓ |
| Library | | | | |
| Access library workspace | ✓ | ✓ | ✓ | ✓ |
| CAC settings | | | | |
| Enable Central Administration | ✓ | × | × | × |
| MS Tune | | | | |
| Access MS Tune workspace | ✓ | ✓ | ✓ | × |
| Advanced MS Tuning | ✓ | ✓ | × | × |
| Advanced troubleshooting | ✓ | ✓ | × | × |
| Quick status check | ✓ | ✓ | ✓ | × |

Access Control

Table 4-5 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|---|---------------|------------------|---------|----------|
| Restore instrument data | ✓ | ✓ | × | × |
| Explorer | | | | |
| Access explorer workspace | ✓ | ✓ | ✓ | ✓ |
| Export | ✓ | ✓ | ✓ | × |
| Print | ✓ | ✓ | ✓ | × |
| Options | ✓ | ✓ | ✓ | × |
| Recalibrate | ✓ | ✓ | × | × |
| Analytics | | | | |
| New results | ✓ | ✓ | ✓ | × |
| Create processing method | ✓ | ✓ | ✓ | × |
| Modify processing method | ✓ | ✓ | × | × |
| 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 | ✓ | × | × | × |
| Add samples | ✓ | ✓ | ✓ | × |

Table 4-5 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|---|---------------|------------------|---------|----------|
| 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 | ✓ | ✓ | ✓ | × |
| 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 | ✓ | × | × | × |

Access Control

Table 4-5 Preset Permissions (continued)


| Permission | Administrator | Method Developer | Analyst | Reviewer |
|--|---------------|------------------|---------|----------|
| 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 | ✓ | ✓ | × | × |
| 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 | ✓ | ✓ | × | × |

Table 4-5 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|--|---------------|------------------|---------|----------|
| 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 software 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 software 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 **Delete a Role**.
The Delete a User Role dialog opens.
5. 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. |
| \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 | <ul style="list-style-type: none"> Workstation audit trail data and archives Workstation audit trail settings Project audit trail data and archives Project audit trail settings | <ul style="list-style-type: none"> For projects: <project name>\Audit Data For the workstation: C:\ProgramData\SCIEX\Audit Data |
| atms | Audit maps | <ul style="list-style-type: none"> For projects: <project name>\Audit Data For the workstation: C:\ProgramData\SCIEX\Audit Data |
| bch | Batch | Batch |

Access Control

Table 4-7 SCIEX OS Files (continued)

| Extension | File Type | Folder |
|-----------|--|--|
| cset | Results Table settings | Project Information |
| dad | Mass spectrometry data file | <ul style="list-style-type: none"> • Optimization • Data |
| exml | Project default settings | Project Information |
| journal | Temporary files created by SCIEX OS | Various folders |
| lcm | LC Method | Acquisition Methods |
| msm | MS Method | Acquisition Methods |
| pdf | Portable document data | — |
| qlayout | Workspace layout | <p>—</p> <hr/> <p>Note: The default workspace layout for a project is stored in the Project Information folder.</p> <hr/> |
| qmethod | Processing method | Quantitation Methods |
| qsession | Results Table <hr/> <p>Note: SCIEX OS can only open qsession files that were created with SCIEX OS.</p> <hr/> | Quantitation Results |
| wiff | Mass spectrometry data file compatible with the SCIEX OS software <hr/> <p>Note: SCIEX OS generates both wiff and wiff2 files.</p> <hr/> | Data |
| wiff.scan | Mass spectrometry data file | <ul style="list-style-type: none"> • Optimization • Data |
| wiff2 | Mass spectrometry data file generated by SCIEX OS | <ul style="list-style-type: none"> • Optimization • Data |

Table 4-7 SCIEX OS Files (continued)

| Extension | File Type | Folder |
|-------------|-------------------|----------|
| xls or.xlsx | Excel spreadsheet | Batch |
| xps | Recalibration | Data\Cal |

The Central Administrator Console (CAC) software is an optional alternative to local administration with the SCIEX OS software. The CAC software contains central role, user, workstation, and workgroup management and customization, all in one application.

This section describes the CAC software and explains how to configure and use it to centrally manage people, projects, and workstations.

Note: To use the CAC software and register workstations with the server, make sure that the SCIEX OS software is installed on each workstation.

The CAC software is license-enabled and can be installed on any workstation that supports SCIEX OS version 3.0 and Windows Server 2019.

The CAC software is a part of the SCIEX OS installer package. However, the CAC software and SCIEX OS cannot be installed on the same workstation.


Users

Use the User Management page to add Windows users and groups to the User Management database for SCIEX OS. The administrator can also add, modify, and delete user roles in the User Roles and Permissions section. 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.

User Pool

Only authorized users can log on to the workstation and access SCIEX OS when SCIEX OS is managed with the Central Administrator Console (CAC) software. Before users can be added to workgroups, they must be added to the user pool.

Add a User or Group to the User Pool

1. Open the Central Administration workspace.
2. Open the User Management page.
3. Open the User Pool tab.
4. Click **Add users to the User Pool** ().
The Select Users or Groups dialog opens.
5. Type the name of a user or group and then click **OK**.

Tip! Press and hold **Ctrl** key and then click **OK** to select multiple users or groups.

Delete Users or Groups

1. Open the Central Administration workspace.
2. Open the User Management page.
3. Open the User Pool tab.
4. In the right pane, select the user or group to be deleted, and then click **Delete**. The software prompts for confirmation.
5. Click **OK**.

User Roles and Permissions

This section describes the User Roles and Permissions page.

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 changed.

Table 5-1 Predefined Roles

| Role | Typical Tasks |
|-------------------------|---|
| Administrator | <ul style="list-style-type: none"> • Manages the system. • Configures security. |
| Method Developer | <ul style="list-style-type: none"> • Creates methods. • Runs batches. • Analyzes data for use by the end-user. |
| Analyst | <ul style="list-style-type: none"> • Runs batches. • Analyzes data for use by the end-user. |
| Reviewer | <ul style="list-style-type: none"> • Reviews data. • Reviews audit trails. • Reviews quantitation results. |

Central Administrator Console

Table 5-2 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 | | | | |
| General tab | ✓ | ✓ | × | × |
| General: change regional setting | ✓ | ✓ | × | × |
| General: full screen mode | ✓ | ✓ | × | × |
| LIMS communication tab | ✓ | ✓ | × | × |
| General: Stop Windows services | ✓ | × | × | × |
| Audit maps tab | ✓ | × | × | × |
| Queue tab | ✓ | ✓ | ✓ | ✓ |
| Queue: instrument idle time | ✓ | ✓ | × | × |
| Queue: max number of acquired samples | ✓ | ✓ | × | × |
| Queue: other queue settings | ✓ | ✓ | × | × |

Table 5-2 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|--|---------------|------------------|---------|----------|
| 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 | ✓ | × | × | × |
| 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 | | | | |

Central Administrator Console

Table 5-2 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|-------------------------------|---------------|------------------|---------|----------|
| Start | ✓ | ✓ | ✓ | × |
| Stop | ✓ | ✓ | ✓ | × |
| Save | ✓ | ✓ | ✓ | × |
| MS & LC Method | | | | |
| Access method workspace | ✓ | ✓ | ✓ | ✓ |
| New | ✓ | ✓ | × | × |
| Open | ✓ | ✓ | ✓ | ✓ |
| Save | ✓ | ✓ | × | × |
| Save as | ✓ | ✓ | × | × |
| Lock/Unlock method | ✓ | ✓ | × | × |
| Queue | | | | |
| Manage | ✓ | ✓ | ✓ | × |
| Start/Stop | ✓ | ✓ | ✓ | × |
| Print | ✓ | ✓ | ✓ | ✓ |
| Library | | | | |
| Access library workspace | ✓ | ✓ | ✓ | ✓ |
| CAC settings | | | | |
| Enable Central Administration | ✓ | × | × | × |
| MS Tune | | | | |
| Access MS Tune workspace | ✓ | ✓ | ✓ | × |
| Advanced MS Tuning | ✓ | ✓ | × | × |
| Advanced troubleshooting | ✓ | ✓ | × | × |
| Quick status check | ✓ | ✓ | ✓ | × |

Table 5-2 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|---|---------------|------------------|---------|----------|
| Restore instrument data | ✓ | ✓ | × | × |
| Analytics | | | | |
| New results | ✓ | ✓ | ✓ | × |
| Create processing method | ✓ | ✓ | ✓ | × |
| Modify processing method | ✓ | ✓ | × | × |
| 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 | ✓ | × | × | × |
| Add samples | ✓ | ✓ | ✓ | × |
| Remove selected samples | ✓ | ✓ | ✓ | × |
| Export, import, or remove external calibration | ✓ | ✓ | ✓ | × |
| Modify sample name | ✓ | ✓ | ✓ | × |
| Modify sample type | ✓ | ✓ | ✓ | × |
| Modify sample ID | ✓ | ✓ | ✓ | × |

Central Administrator Console

Table 5-2 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|---|---------------|------------------|---------|----------|
| Modify actual concentration | ✓ | ✓ | ✓ | × |
| Modify dilution factor | ✓ | ✓ | ✓ | × |
| Modify comment fields | ✓ | ✓ | ✓ | × |
| Enable manual integration | ✓ | ✓ | ✓ | × |
| 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 | ✓ | × | × | ✓ |

Table 5-2 Preset Permissions (continued)


| Permission | Administrator | Method Developer | Analyst | Reviewer |
|--|---------------|------------------|---------|----------|
| Modify report template | ✓ | ✓ | × | × |
| Transfer results to LIMS | ✓ | ✓ | ✓ | × |
| Modify barcode column | ✓ | ✓ | × | × |
| Change comparison sample assignment | ✓ | ✓ | × | × |
| 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 | ✓ | × | × | × |
| Explorer | | | | |

Table 5-2 Preset Permissions (continued)

| Permission | Administrator | Method Developer | Analyst | Reviewer |
|---------------------------|---------------|------------------|---------|----------|
| Access explorer workspace | ✓ | ✓ | ✓ | ✓ |
| Export | ✓ | ✓ | ✓ | × |
| Print | ✓ | ✓ | ✓ | × |
| Options | ✓ | ✓ | ✓ | × |
| Recalibrate | ✓ | ✓ | × | × |

Add a Custom Role

The Central Administrator Console (CAC) software has four predefined roles. If additional roles are required, then copy an existing role and assign access rights.

1. Open the Central Administration workspace.
2. Open the User Management page.
3. Open the User Roles and Permissions 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**.
The new role is shown in the User Roles and Permission Categories window.
7. Select the access privileges for the role by selecting the appropriate check boxes.
8. Click **Save All Roles**.

Delete a Custom Role

1. Open the Central Administration workspace.
2. Open the User Management page.
3. Open the User Roles and Permissions tab.
4. Click **Delete a Role**.
The Delete a User Role dialog opens.
5. Select the role to be deleted and then click **OK**.

Workgroups

Use the Workgroup Management page to manage workgroups. Workgroups have users, workstations, and projects.

Create a workgroup by adding resources from their respective pools. Before creating any workgroups, make sure to add all potential users to the User Pool, workstations to the Workstation Pool, and project root directories to the Project Pool.

If required, add additional roles. Optionally, select the security mode for each workgroup.


The security mode setting for the workgroup takes precedence over the security mode setting for the workstation if the workstation is registered with the Central Administrator Console (CAC) software and if it is a member of the workgroup.

Do not add local users to workgroups. The CAC software is a network application and only network users should be added to a workgroup.

Note: In each workgroup, at least one user must be assigned the administrator role. Only an administrator or supervisor can unlock the CAC software screen if the currently logged on user is unavailable.

If server-based security is no longer required for a particular workstation, then manage security for the workstation locally with SCIEX OS.

Create a Workgroup

1. Open the Central Administration workspace.
2. Open the Workgroup Management page.
3. Click **Add Workgroup** ().
The Add a Workgroup dialog opens.
4. Type a name in the **Workgroup Name** field.
5. Type a description in the **Description** field, and then click **Add**.
The workgroup is created and added to the Manage Workgroups and Assignments pane.
The Central Administrator Console (CAC) software creates the appropriate workgroup name on the server.

Note: Integrated mode is the default security setting.


Delete a Workgroup

If a workgroup is no longer required, then delete it from the Workgroup list. Deleting a workgroup only deletes the workgroup from the Central Administrator Console (CAC) software. No data is lost from the workstation.

1. Open the Central Administration workspace.
2. Open the Workgroup Management page.
3. Expand the **Workgroups** list and find the workgroup to be deleted. Click **Delete**. The Delete Workgroup dialog opens.
4. Click **Yes**.

Add Users or Groups to a Workgroup

Note: Users added to the workgroup are not automatically assigned a role. To assign roles to users, refer to the section: [Add or Remove a Role](#).

1. Open the Central Administration workspace.
2. Open the Workgroup Management page.
3. In the Manage Workgroups and Assignments pane, expand the workgroup to be changed and then expand the **Users** list.
4. Select a user or group and then click **Add** ().

Tip! Add or select multiple users by pressing **Shift** and then selecting the required users.

The user or group is added to the current workgroup.

5. Assign one or more roles to the added user or group. Refer to the section: [Add or Remove a Role](#).
6. Click **Save**.

Add or Remove a Role

| Prerequisite Procedures |
|---|
| <ul style="list-style-type: none">• Add Users or Groups to a Workgroup. |


For information about creating roles in the Central Administrator Console (CAC) software, refer to the section: [Add a Custom Role](#). Users or groups with an assigned role have all the permissions associated with the role. Users or groups can have more than one role at a time.

1. Open the Central Administration workspace.
-

2. Open the Workgroup Management page.
3. In the Manage Workgroups and Assignments pane, expand the workgroup to be changed and then expand the **Users** list.
4. In the Current Workgroup Membership section, assign or remove roles in the **Assign Roles** column.
5. Click **Save**.

Add Workstations to a Workgroup

Note: A workstation is shown in the workstation pool only if it has been registered with the Central Administrator Console (CAC) software. Refer to the section: [Add a Workstation](#)

1. Open the Central Administration workspace.
2. Open the Workgroup Management page.
3. In the Manage Workgroups and Assignments pane, expand the workgroup to be changed, and then expand the **Workstations** list.
4. Select a workstation and then click **Add** ().
The workstation is added to the current workgroup.
5. Click **Save**.

Assign Workgroup Security Settings

| Prerequisite Procedures |
|---|
| <ul style="list-style-type: none">• Add a Workstation• Add Workstations to a Workgroup |


For information on security modes, refer to the section: [Configure the Security Mode](#).

1. Open the Central Administration workspace.
2. Open the Workgroup Management page.
3. In the Manage Workgroups and Assignments pane, expand the workgroup to be changed, and then expand the **Workstations** list.
4. (Optional) To make the current workgroup the default workgroup for that workstation, select the **Set Default** check box in the Current Workgroup Membership section.
5. In the Assign Security Settings section, select the **Security mode** for the workgroup and then type the appropriate **Screen lock** and **Auto logoff** times.
6. Click **Save**.

Add Projects to a Workgroup

Note: This procedure is only required if project access is managed centrally.

Note: If a project is added to more than one workgroup, then user access to the project is appended, not overwritten. For example, Workgroup 1 has User A, User B, and Project_01. Workgroup 2 has User B and User C. If Project_01 is added to Workgroup 2, then User A, User B, and User C will all have access to Project_01.

1. Open the Central Administration workspace.
2. Open the Workgroup Management page.
3. In the Manage Workgroups and Assignments pane, expand the workgroup to be changed, and then expand the **Projects** list.
4. Select the **Use central settings for projects** check box.
The project selection section is shown.
5. Select a **Project root directory** to add an entire group of projects, or expand the project root and select a specific project to add to the workgroup.
6. Click **Add** () to add the projects to the workgroup.
The project root is added to the Current Workgroup Membership table. Expand the project root to show the current projects in the workgroup.
7. Click **Save**.

Manage Projects

Use the Project Management page to create, modify, and delete projects.

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: [About Projects and Root Directories](#).

About Projects and Root Directories

A root directory is a folder that contains one or more projects. It is the folder in which the software looks for project data. The predefined root directory is `D:\SCIEX OS Data`.

To make sure that project information is stored safely, create projects using the Central Administrator Console (CAC) software. Add projects to the Project Root Pool before adding them to a workgroup. Refer to the section: [Add a Project](#).

Project data can be organized in subfolders. Create the subfolders with the CAC software. Refer to the section: [Add a Subfolder](#).


Note: If a project is created outside of the CAC software, then the project root should be refreshed after the project is created. When the root is refreshed, the contents of the Project Root Pool are synchronized with the contents of the project roots on the network.

Add a Root Directory

A root directory is the folder in which one or more projects are stored.

Note: The software saves up to ten root directories.

Tip! Local drives are not accessible on the network. A root directory can only be created on a shared drive.

1. Open the Central Administration workspace.
 2. Open the Project Management page.
 3. Click **Add new or existing project root to project pool** ().
The Add Root Directory dialog opens.
 4. Type the full path to the root directory folder and then click **OK**.
The folder is created.
-

Tip! Instead of typing the path, click **Browse**, and then select the folder in which the root directory will be created.

Tip! Alternatively, create a folder in File Explorer, and then browse to and select the folder.

Note: For SCIEX OS installations with a processing license, the root directory can be an Analyst software (`Analyst Data\Projects`) folder.

5. Click **OK**.
The new root directory becomes the root directory for the current project.
-

Delete a Project Root Directory

The software keeps a list of the last ten root directories that were used. The user can delete root directories from this list.

Note: Deleting a project root directory also deletes all associated projects from the project root pool.

1. Open the Central Administration workspace.
 2. Open the Project Management page.
-

Central Administrator Console

3. Find the project root directory to be deleted, and then click **Delete Project Root** in the Actions section.
The software prompts for confirmation.
4. Click **OK**.

Add a Project

| Prerequisite Procedures |
|--|
| <ul style="list-style-type: none">• Add a Root Directory |


The project stores acquisition methods, data, batches, processing methods, processing results, and so on. We recommend the use of a separate project folder for each project.

Do not create projects or copy or paste files outside of the Central Administrator Console (CAC) software.

1. Open the Central Administration workspace.
2. Open the Project Management page.
3. Click **Add project** in the Actions section of the root folder.
The New Project dialog opens.
4. Type the project name.
5. Click **OK**.
The new project is shown under the project root.

Add a Subfolder

Data in projects can be further organized in subfolders.

1. Open the Central Administration workspace.
2. Open the Project Management page.
3. Click **Add data sub-folders** in the Actions section of the root folder.
The Add Data Sub-Folders dialog opens.
4. Select a project to which the subfolder will belong.
5. Click **Add a new data sub-folder** ().
The Data Sub-Folder Name dialog opens.
6. Type the name of the subfolder.
7. Click **Save**.

Tip! Subfolders can be nested within other subfolders. To create a nested subfolder, select an existing subfolder in the Project Data Sub-Folders section and then click **Add a new**

data sub-folder ().


8. Close the Add Data Sub-Folders dialog.

Workstations

Use the Workstation Management page to manage all workstations connected to the CAC server. Workstations under the control of the CAC software automatically have customized settings applied to them.

Add a Workstation

On the Workstation Management page, administrators can add or remove workstations from the control of the Central Administrator Console (CAC) software.

1. Open the Central Administration workspace.
2. Open the Workstation Management page.
3. Click **Add Workstation to the Workstations Pool** ().
The Select Computers dialog opens.
4. Type the names of the workstations to be added and then click **OK**.

Delete a Workstation

If a workstation is no longer in use or if it is no longer required to be part of a workgroup, then delete it from the workstation pool. Deleting a workstation removes it from any workgroups to which it was assigned. No data is lost on the workstation when it is removed.

1. Open the Central Administration workspace.
2. Open the Workstation Management page.
3. Click **Workstation Management**.
4. In the Workstation Pool pane, find the workstation to be deleted, and then click **Delete**.
The Delete Workstation dialog opens.
5. Click **OK**.

Reports and Security Features

Generate Workgroup Data Reports

Users can generate data reports that include details like configured users, roles, workstations, projects, and workgroups.

1. Open the Central Administration workspace.
2. Click **Print**.
The Print dialog opens.
3. Set the printing options and then click **Print**.
4. (Print to PDF only) Browse to the location in which the Report will be saved and then click **Save**.

Export CAC Software Settings

The user can export security settings that can be applied to another Central Administrator Console (CAC) server. The settings are exported as an ecac file.

1. Open the Central Administration workspace.
2. Click **Advanced > Export CAC settings**.
The Export CAC Settings dialog opens.
3. Click **Browse**.
4. Browse to and select the folder where the settings will be saved, and then click **Select Folder**.
5. Click **Export**.
A confirmation message is shown, with the name of the file that contains the exported settings.
6. Click **OK**.

Import CAC Software Settings

| |
|--|
| Prerequisite Procedures |
| <ul style="list-style-type: none">• Export CAC Software Settings |

The user can import security settings from SCIEX OS or other Central Administrator Console (CAC) servers. The settings are imported from an ecac file.

1. Open the Central Administration workspace.
2. Click **Advanced > Import CAC settings**.

The Import CAC Settings dialog opens.

3. Click **Browse**.
4. Browse to and select the file that contains the settings to be imported, and then click **Open**. The software makes sure that the file is valid.
5. Click **Import**.
The software backs up the current settings and then imports the new settings. A confirmation message is shown.

Note: The imported settings are applied after the CAC software is restarted.

6. Click **OK**.

Restore CAC Software Settings

The user can automatically import the last exported ecac settings.

1. Open the Central Administration workspace.
2. Click **Advanced > Restore CAC settings**.
The Restore CAC Settings dialog opens.

Note: The restored settings are applied after the Central Administrator Console (CAC) software is restarted.

3. Click **Yes**.

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**.

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

Audit Trails

Audited events are stored in audit trails. Two types of audit trail are available: workstation and project.

Workstation audit trails are files that store the audited events for the computer on which SCIEX OS or the Central Administrator Console (CAC) software is running. For a complete list of audited events, refer to the section: [Workstation Audit Trail](#).

A project audit trail is the file that stores the audited events for project. For a complete list of audited events, refer to the section: [Project Audit Trail](#). In SCIEX OS and the CAC software, the Audit Trail workspace shows the audit trails for the projects in the current root directory. 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 7-1 Audit Trails

| Audit Trail | Examples of Events Recorded | Available Audit Maps Stored In | Default Audit Maps |
|------------------------|--|---|--|
| Workstation (SCIEX OS) | <ul style="list-style-type: none">• Changes to:<ul style="list-style-type: none">• Active audit map assignment• Instrument tuning• Sample queues• Security• Tuning• Devices | <ul style="list-style-type: none">• C:\ProgramData\SCIEX\ Audit Data folder | <ul style="list-style-type: none">• No Audit Map |

Auditing

Table 7-1 Audit Trails (continued)

| Audit Trail | Examples of Events Recorded | Available Audit Maps Stored In | Default Audit Maps |
|---------------------------|--|---|---|
| Workstation (CAC) | <ul style="list-style-type: none">• Changes to:<ul style="list-style-type: none">• Audit map• CAC server• Security• User log | <ul style="list-style-type: none">• C:\ProgramData\SCIEX\ Audit Data folder | <ul style="list-style-type: none">• Silent Audit Map |
| Project (one per project) | <ul style="list-style-type: none">• Changes to:<ul style="list-style-type: none">• Active audit map assignment (SCIEX OS)• Project• Data• Printing | <ul style="list-style-type: none">• <project>\Audit Data folder | <ul style="list-style-type: none">• 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 and the CAC software automatically archives the records and begins a new audit trail. For more information, refer to the section: [Audit Trail Archives](#).

Audit Maps

An audit map is a file that contains a list of all of the events that can be audited, and whether a reason for change or electronic signature is required for the event. Two types of audit maps are available: workstation and project.

Workstation audit maps control the events that are audited on a workstation.

Project audit maps control the events that are audited for a project, and are stored in the project folder.

Note: The audit map for a project can be edited in either SCIEX OS or the Central Administrator Console (CAC) software.

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.

When SCIEX OS is installed, the default audit map for all new projects is No Audit Map. When the CAC software is installed, the default audit map for all new projects is Silent Audit Map. 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 the software 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 7-2 Checklist for Configuring Auditing

| Task | Refer To |
|---|--|
| Create an audit map for the workstation audit trail. | <ul style="list-style-type: none"> Create a Workstation Audit Map. Edit a Workstation Audit Map. |
| Apply the audit map to the workstation audit trail. | <ul style="list-style-type: none"> Change the Active Audit Map for a Workstation. |
| Create a default active audit map for new projects. | <ul style="list-style-type: none"> Create a Project Audit Map. |
| Configure the audit map to be used for each existing project. | <ul style="list-style-type: none"> Create a Project Audit Map. Edit a Project Audit Map. |
| Apply an audit map to each existing project. | <ul style="list-style-type: none"> 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 7-3 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. |

Auditing

Table 7-3 Installed Audit Maps (continued)

| Audit Map | Description |
|------------------|---|
| 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 7-1](#). 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 7-2](#).

Work with Audit Maps


The software 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 the software 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. Open 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. Open 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**.

Auditing

- 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. Open 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. Open 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. Open 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. Open 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. Open 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. Open 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 describes the fields in the audit trail records.

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 7-4 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. |

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](#).

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.

Access Data During Network Disruptions

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`.

Note: The default audit map for new projects created in the Central Administrator Console (CAC) software is the **Silent Audit Map**.

Project audit trail events are shown in both the CAC software and SCIEX OS.

Table B-1 Project Audit Trail Events

| SCIEX OS or CAC | Analyst Software |
|---|---|
| Analytics Workspace | |
| Actual Concentration changed | Quantitation Events: 'Concentration' has been changed |
| Auto-Processing File saved | — |
| Barcode ID changed | — |
| Comparison sample changed in non-targeted workflow | — |
| Custom columns modified | Quantitation Events: 'Custom Title' has changed |
| Data exploration opened | Project Events: Data File has been opened |
| Data exported | — |
| Data transferred to LIMS | — |
| Dilution Factor changed | Quantitation Events: 'Dilution Factor' has been changed |
| External calibration changed | — |
| External calibration exported | — |

Audit Events

Table B-1 Project Audit Trail Events (continued)

| SCIEX OS or CAC | Analyst Software |
|--|--|
| File saved | Project Events: Quantitation Results Table has been created, Quantitation Results Table has been modified, Quantitation Events: Results Table has been saved |
| 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 |
| Integration cleared | — |
| Integration parameters changed | Quantitation Events: Quantitation peak has been integrated |
| Library search result changed | — |
| Manual Integration | Quantitation Events: Quantitation Peak has been integrated |
| Manual Integration reverted | Quantitation Events: Quantitation peak has been reverted back to original |
| MS/MS selection changed | — |
| Processing method changed and applied | Quantitation Events: Quantitation method has been changed |
| Report created | Project Events: Printing document on printer, Finished printing document on printer |
| Results Table approved | Quantitation Events: QA reviewer has accessed a results table |
| Results Table created | Quantitation Events: Results table has been created |
| Results Table locked | — |
| Results Table unlocked | — |
| Sample ID changed | Quantitation Events: 'Sample ID' has been changed |
| Sample Name changed | Quantitation Events: 'Sample Name' has been changed |

Table B-1 Project Audit Trail Events (continued)

| SCIEX OS or CAC | Analyst Software |
|--|---|
| 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 |
| Sample Type changed | Quantitation Events: 'Sample Type' has been changed |
| Std. Addition Actual concentration changed | — |
| Used column selection changed | Quantitation Events: 'Use It' has been changed |
| Window/pane printed | Project Events: Printing document on printer, Finished printing document on printer |
| 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 |
| Explorer Workspace | |
| Open Sample(s) | Project Events: Data File has been opened |
| Recalibrate sample(s) | — |
| Recalibrate sample(s) started | — |
| LC Method Workspace | |
| 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 |

Audit Events

Table B-1 Project Audit Trail Events (continued)

| SCIEX OS or CAC | Analyst Software |
|--------------------|------------------|
| 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`.

Note: The default audit map for new workstations in the Central Administrator Console (CAC) software is the **Silent Audit Map**.

Workstation audit trail events are shown in both the CAC software and SCIEX OS.

Table B-2 Workstation Audit Trail Events

| SCIEX OS or CAC | Analyst Software |
|--|---|
| Instrument Tune (SCIEX OS) | |
| 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 (SCIEX OS) | |
| Devices Activated | Instrument Events: Hardware profile has been activated |
| Devices Deactivated | Instrument Events: Hardware profile has been deactivated |
| Data File Checksum (SCIEX OS) | |
| Wiff data file checksum has been changed | — |
| Explorer Workspace (SCIEX OS) | |
| Open Sample(s) | Project Events: Data File has been opened |

Table B-2 Workstation Audit Trail Events (continued)

| SCIEX OS or CAC | Analyst Software |
|--|---|
| Recalibrate samples(s) | — |
| Recalibrate samples(s) started | — |
| Audit Map Page¹ | |
| Workstation Audit Map changed | Instrument Events: Instrument Settings have been changed |
| Workstation Audit Trail printed | — |
| Workstation Audit Trail exported | — |
| CAC Server (CAC) | |
| Project settings enabled/disabled in a workgroup | — |
| Project assigned/unassigned to a workgroup | — |
| User Role(s) assigned/unassigned to user(s) in workgroup | — |
| User(s)/UserGroup(s) assigned/unassigned to a workgroup | — |
| Workgroup added/deleted | — |
| Workgroup renamed | — |
| Workstation(s) assigned/unassigned to a workgroup | — |
| Queue Workspace (SCIEX OS) | |
| 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 |
| Reacquiring sample | Instrument Events: Reacquiring sample(s) |
| Sample starts to acquire | — |
| Print Queue | Project Events: Printing Document on printer, Finished printing document on printer |

¹ These events are recorded in both SCIEX OS and CAC.

Audit Events

Table B-2 Workstation Audit Trail Events (continued)

| SCIEX OS or CAC | Analyst Software |
|--|---|
| Sample acquisition has completed | Project Events: Sample has been added to Data file |
| Automatic reinjections Occurred | — |
| Automatic injection Occurred | — |
| Security¹ | |
| Auto logoff by system | Instrument Events: User Logged out |
| Forced logoff by another user | Instrument Events: User Logged out |
| Forced Logoff failed | — |
| Screen unlock failed | — |
| Secure Network Account credentials have been changed | Instrument Events: Acquisition Account Changed |
| Secure Network Account credentials have been removed | Instrument Events: Acquisition Account Changed |
| Secure Network Account credentials have been specified | Instrument Events: Acquisition Account Changed |
| Security configuration changed | Instrument Events: The Security Configuration has been modified, Screen Lock Changed, Auto Logout changed |
| User added/deleted | Instrument Events: User Added, User Deleted |
| User has logged in | Instrument Events: User Logged In |
| User has logged out | Instrument Events: User Logged out |
| User has turned off exclusive mode | — |
| User Login Failed | Instrument Events: User Login Failed |
| User management settings have been exported | — |
| User management settings have been imported | — |
| User management settings have been restored | — |
| User role assigned to user/user group | Instrument Events: User Changed User Type |
| User role deleted | Instrument Events: User Type Deleted |

Table B-2 Workstation Audit Trail Events (continued)

| SCIEX OS or CAC | Analyst Software |
|----------------------|--------------------------------------|
| User role modified | Instrument Events: User Type Changed |
| UserLog ¹ | |
| Print Event Log | — |

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 | — |
| General: Stop Windows services | — |
| 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 | — |
| Queue: other queue settings | — |

Mapping of Permissions Between SCIEX OS and the Analyst Software

Table C-1 Permission Mapping (continued)

| SCIEX OS | Analyst Software |
|---|---|
| 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 | — |
| New | Acquisition Method: Create/Save acquisition method |

Mapping of Permissions Between SCIEX OS and the Analyst Software

Table C-1 Permission Mapping (continued)

| SCIEX OS | Analyst Software |
|-------------------------------|--|
| 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 |
| CAC settings | |
| Enable Central Administration | — |
| MS Tune Workspace | |
| Access MS Tune workspace | — |
| Advanced MS tuning | Tune: Instrument Optimization, Manual Tune, Edit Tuning Options |
| Advanced troubleshooting | — |
| Quick status check | Tune: Instrument Opt |
| Restore instrument data | Tune: Edit Tuning Options, Edit instrument data |
| Explorer Workspace | |
| Access explorer workspace | — |

Mapping of Permissions Between SCIEX OS and the Analyst Software

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 | — |
| 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 |

Mapping of Permissions Between SCIEX OS and the Analyst Software

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 | — |

Mapping of Permissions Between SCIEX OS and the Analyst Software

Table C-1 Permission Mapping (continued)

| SCIEX OS | Analyst Software |
|--|--|
| 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 | 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 wiff 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 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.

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

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

Contact Us

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