SCIEX
The Power of Precision

SCIEX OS Software

Handbuch für Laborleiter

RUO-IDV-05-7370-DE-I

Juni 2022

Nur für Forschungszwecke. Nicht zur Verwendung bei Diagnoseverfahren.

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

Inhalt

Einleitung 1

Die in diesem Handbuch enthaltenen Informationen richten sich an zwei primäre Zielgruppen:

- Den Laborleiter, der sich mit dem täglichen Betrieb und der Nutzung der SCIEX OS Software und den dazu gehörenden Instrumenten aus funktionaler Sicht befasst.
- Systemadministratoren, die sich mit der Sicherheit des Systems und mit der System- und Datenintegrität befassen.

Übersicht über die Sicherheitskonfiguration 2

In diesem Abschnitt wird beschrieben, wie die Komponenten von SCIEX OS für Zugriffskontrolle und Auditing in Verbindung mit den Windows-Komponenten für Zugriffskontrolle und Auditing arbeiten. Außerdem wird die Konfiguration der Windows-Sicherheit vor der Installation von SCIEX OS beschrieben.

Sicherheit und Einhaltung gesetzlicher Vorschriften

SCIEX OS bietet:

- Anpassbare Verwaltung, um den Bedürfnissen von Forschung und regulatorischen Anforderungen gerecht zu werden.
- Sicherheits- und Prüfwerkzeuge für die Unterstützung der Konformität nach 21 CFR Part 11 für die Verwendung von elektronischen Aufzeichnungen.
- Flexible und effiziente Verwaltung des Zugangs zu kritischen Massenspektrometer-Funktionen.
- Kontrollierter und geprüfter Zugriff auf wichtige Daten und Berichte.
- Einfache Sicherheits-Management-Anbindung an Windows-Sicherheit.

Sicherheitsanforderungen

Die Sicherheitsanforderungen reichen von relativ offenen Umgebungen wie in Forschungs- oder akademischen Labors bis hin zu extrem streng geregelten Umgebungen wie jene in forensischen Labors.

SCIEX OS und Windows Security: Zusammenarbeit

SCIEX OS und das Windows New Technology File System (NTFS) verfügen über Sicherheitsfunktionen, um den System- und Datenzugriff zu kontrollieren.

Die Windows-Sicherheit bietet die erste Schutzebene, indem von Nutzern verlangt wird, sich am Netzwerk mit einem eindeutigen Benutzernamen und Passwort anzumelden. Das führt dazu, dass nur Benutzer, die von den lokalen Windows-Sicherheitseinstellungen oder von den Windows-Netzwerkeinstellungen erkannt werden, Zugriff auf das System erhalten. Weitere Informationen finden Sie im Abschnitt: Windows-Sicherheitskonfiguration.

SCIEX OS hat die folgenden Zugriffsmodi auf das Sicherheitssystem:

- „Mixed Mode“ (Gemischter Modus)
- „Integrated Mode“ (Integrierter Modus) (Standardeinstellung)

Weitere Informationen über Sicherheitsmodi und Sicherheitseinstellungen finden Sie im Abschnitt: Konfigurieren des Sicherheitsmodus.

SCIEX OS vollständig konfigurierbare Rollen, die von den mit Windows verbundenen Benutzergruppen getrennt sind. Durch die Verwendung von Rollen kann der Laborleiter den Zugriff auf die Software und das Massenspektrometer auf der Grundlage der Funktion steuern. Weitere Informationen finden Sie im Abschnitt: Konfiguration des Zugriffs auf SCIEX OS.

Audit-Trails innerhalb von SCIEX OS und Windows

Die Auditing-Funktionen innerhalb von SCIEX OS sowie die integrierten Windows-Auditing-Komponenten sind für die Erstellung und Verwaltung von elektronischen Aufzeichnungen entscheidend.

SCIEX OS bietet ein System von Audit-Trails, das die Anforderungen an elektronische Aufzeichnungen erfüllt. Separate Audit-Trail-Aufzeichnungen:

- Änderungen von Massenkalibrierungstabellen oder Auflösungstabellen, Änderungen der Systemkonfiguration und sicherheitsrelevante Ereignisse.
- Erstellungs- und Änderungsereignisse für Projekte, Tuning, Chargen, Daten, Verarbeitungsmethoden und Berichtvorlagendateien sowie das Öffnen und Schließen von Modulen und Druckereignisse. Zu den Löschereignissen, die im Audit-Trail aufgezeichnet werden, gehören das Löschen von Rollen und Benutzern in SCIEX OS.
- Erstellung und Änderung der Probeninformationen, Peak-Integrations-Parameter und integrierten Verarbeitungsmethode in einer „Results Table“.

Hinweis: SCIEX OS prüft nicht die Erstellung von bzw. Änderungen an MS-Methoden, LC-Methoden, Chargen oder Verarbeitungsmethoden. Diese Dateien fungieren als Vorlagen. Parameterwerte werden bei der Erfassung oder Verarbeitung aus diesen gelesen und auf die Task angewendet. Bei MS-Methoden, LC-Methoden und Chargen werden die Parameterwerte in den .wiff- und .wiff2-Dateien aufgezeichnet. Bei Verarbeitungsmethoden werden sie in der qsession-Datei aufgezeichnet. Diese Dateien dienen als elektronische Datensätzen für diese Informationen.

Eine vollständige Liste der Audit-Ereignisse finden Sie im Abschnitt: Audit-Ereignisse.

SCIEX OS verwendet Folgendes: Anwendungsereignisprotokoll, um Informationen über den Betrieb der Software zu erfassen. Verwenden Sie dieses Protokoll als Hilfe bei der Fehlerbehebung. Es beinhaltet detaillierte Informationen über Interaktionen von Massenspektrometer, Geräten und Software.

Windows verwaltet Ereignisprotokolle, die eine Reihe von Sicherheits-, System- und anwendungsspezifischen Ereignissen erfassen. In den meisten Fällen ist die Windows-Überwachung so ausgelegt, dass außergewöhnliche Ereignisse erfasst werden, wie beispielsweise ein Fehler beim Anmelden. Der Administrator kann das System so konfigurieren, dass eine breite Palette von Ereignissen erfasst wird, wie z. B. der Zugriff auf bestimmte Dateien oder administrative Tätigkeiten unter Windows. Weitere Informationen finden Sie im Abschnitt: System-Audits.

Sicherheitsrichtlinien für Kunden: Sicherungen

Die Sicherung der Kundendaten liegt in der Verantwortung des Kunden. SCIEX Service- und Support-Mitarbeiter stehen für Ratschläge und Empfehlungen bezüglich der Sicherung der Kundendaten zur Verfügung, es liegt jedoch in der Verantwortung des Kunden, sicherzustellen, dass die Daten entsprechend den Richtlinien, Anforderungen und den gesetzlichen Anforderungen des Kunden gesichert werden. Häufigkeit und Umfang der Sicherung der Kundendaten sollte den organisatorischen Anforderungen und der Kritikalität der generierten Daten entsprechen.

Kunden sollten sicherstellen, dass die Sicherungen fehlerfrei funktionieren, da Sicherungen ein wesentlicher Bestandteil der gesamten Datenverwaltung und wichtig für die Wiederherstellung im Falle eines böswilligen Angriffs, Hardwarefehlers oder Softwarefehlers sind. Erstellen Sie keine Sicherungen während der Datenerfassung oder stellen Sie sicher, dass die Daten, die gerade erfasst werden, von der Sicherungssoftware ignoriert werden. Es wird dringend empfohlen, eine vollständige Sicherung des Computers vorzunehmen, bevor Sicherheits-Updates installiert oder Reparaturen am Computer durchgeführt werden. Dies vereinfacht ein Rollback in dem seltenen Fall, dass sich ein Sicherheitspatch auf die Funktionsfähigkeit einer Anwendung auswirkt.

21 CFR Teil 11

SCIEX OS umfasst die technische Kontrolle zur Unterstützung von 21 CFR Teil 11 und implementiert dafür Folgendes:

- Verknüpfung der Sicherheit der Modi „Mixed“ (gemischt) und „Integrated“ (integriert) mit der Windows-Sicherheit
- Kontrollierter Zugriff auf Funktionen über anpassbare Rollen
- Audit-Trails für den Gerätebetrieb, die Datenerfassung, Datenprüfung und Berichterstellung
- Elektronische Signaturen aus einer Kombination von Benutzer-ID und Passwort
- Die ordnungsgemäße Konfiguration des Windows-Betriebssystems
- Ordnungsgemäße Verfahren und Schulungen innerhalb des Unternehmens

SCIEX OS wurde als Teil eines mit 21 CFR Teil 11 konformen Systems entwickelt und kann für die Unterstützung der Konformität mit 21 CFR Teil 11 konfiguriert werden. Ob die Nutzung von SCIEX OS mit 21 CFR Teil 11 konform ist oder nicht, hängt von der tatsächlichen Nutzung und Konfiguration von SCIEX OS im Labor ab.

Validierungsdienste stehen über SCIEX Professional Services zur Verfügung. Für weitere Informationen kontaktieren Sie complianceservices@sciex.com.

Hinweis: Belassen Sie die Instrument Parameters Converter Software nicht auf einem validierten System. Sie ist vorgesehen für den ersten Transfer der Instrumenteneinstellungen von der Analyst-Software zu SCIEX OS. Stellen Sie sicher, dass die Instrument Parameters Converter Software von Ihrem Computer entfernt wird, nachdem sie verwendet wurde.

Systemkonfiguration

Die Systemkonfiguration wird in der Regel durch Netzwerkadministratoren oder Personen mit Netzwerk- und lokalen Administrationsrechten durchgeführt.

Windows-Sicherheitskonfiguration

Das System implementiert die folgenden Einschränkungen für die lokalen Windows-Benutzerkonten:

- Das Windows-Passwort muss alle 90 Tage geändert werden.
- Das Windows-Passwort kann für mindestens eine folgende Iteration nicht mehr verwendet werden. Das bedeutet, dass das neue Passwort nicht das unmittelbar vorhergehende Passwort sein darf.
- Das Windows-Passwort muss mindestens acht Zeichen umfassen.
- Das Windows-Passwort muss mindestens zwei der folgenden Anforderungen erfüllen, um den Komplexitätsvorgaben zu entsprechen:
  - Ein Buchstabe in Großschreibung
  - Ein Buchstabe in Kleinschreibung
  - Ein numerischer Wert
  - Ein Sonderzeichen (wie beispielsweise: ! @ # $ % ^ &)
- Der Windows-Benutzername darf nicht **admin**, **administrator** oder **demo** sein.

Der SCIEX OS-Administrator muss die Berechtigung zum Ändern der Dateiberechtigungen für den SCIEX OS-Datenordner haben. Wenn sich dieser Ordner auf einem lokalen Computer befindet, empfiehlt es sich, dass der Software-Administrator Teil der lokalen Administratoren-Gruppe ist.

Um sicherzustellen, dass für die Netzwerkerfassung alle Benutzer über den Zugriff auf die erforderlichen Ressourcen verfügen, kann der Netzwerk-Administrator ein sicheres Netzwerkkonto (SNA) für die Netzwerkressource definieren. Dieses Konto muss über Schreibzugriff für den Netzwerkordner verfügen, der das Stammverzeichnis enthält. Es wird in den Eigenschaften des Stammverzeichnisses als sicheres Netzwerkkonto (SNA) festgelegt.

Benutzer und Gruppen

SCIEX OS verwendet die Benutzernamen und Passwörter, die in der „Primary Domain Controller Security“-Datenbank oder in Active Directory erfasst sind. Passwörter werden mit den von Windows zur Verfügung gestellten Tools verwaltet. Für weitere Informationen über das Hinzufügen und Konfigurieren von Personen und Rollen siehe Abschnitt: Konfiguration des Zugriffs auf SCIEX OS.

Unterstützung von Active Directory

Beim Hinzufügen von Benutzern im Arbeitsbereich „Configuration“ von SCIEX OS geben Sie die Benutzerkonten im UPN-Format (User Principal Name) an. Die folgenden Versionen von Active Directory werden unterstützt:

- Windows 2012 Server
- Windows 7, 64-Bit-Clients
- Windows 10, 64-Bit-Clients

Windows-Dateisystem

In SCIEX OS müssen sich die Dateien und Verzeichnisse auf einer Festplattenpartition im NTFS-Format befinden, die den Zugriff auf SCIEX OS-Dateien steuern und überwachen kann. Das FAT-Dateisystem (FAT = File Allocation Table) kann den Zugriff auf Ordner oder Dateien nicht steuern oder überwachen und ist daher für eine sichere Umgebung nicht geeignet.

Datei- und Ordnerberechtigungen

Zur Verwaltung der Sicherheit muss der SCIEX OS-Administrator das Recht haben, Berechtigungen für den Ordner „`SCIEX OS Data`“ zu ändern. Der Zugang muss durch den Netzwerkadministrator eingerichtet werden.

Hinweis: Beziehen Sie dabei den Grad des Zugriffs, den die Benutzer auf das Laufwerk, das Stammverzeichnis und die Projektordner auf den einzelnen Computern benötigen, in die Überlegungen mit ein. Konfigurieren Sie Sharing (gemeinsame Nutzung) und die damit verbundenen Berechtigungen. Weitere Informationen über File-Sharing finden Sie in der Windows-Dokumentation.

Weitere Informationen über die Datei- und Ordner-Berechtigungen von SCIEX OS finden Sie im Abschnitt: Zugriffssteuerung.

System-Audits

Die Überwachungsfunktion von Windows kann aktiviert werden, um Sicherheitsverletzungen oder Systemeinbrüche festzustellen. Die Auditierung (Überwachung) kann so eingestellt werden, dass verschiedene Arten von systembezogenen Ereignissen aufgezeichnet werden. Beispielsweise kann die Überwachungsfunktion aktiviert werden, um fehlgeschlagene oder erfolgreiche Anmeldeversuche im System im Ereignisprotokoll aufzuzeichnen.

Ereignisprotokolle

Der Windows Event Viewer zeichnet die überwachten Ereignisse im Sicherheits-, System- oder Anwendungsprotokoll auf.

Passen Sie die Ereignisprotokolle wie folgt an:

- Konfigurieren Sie eine geeignete Größe für das Ereignisprotokoll.
- Aktivieren Sie das automatische Überschreiben von alten Ereignissen.

- Aktivieren Sie die Windows-Sicherheitseinstellungen.

Es kann ein Prozess für die Überprüfung und Speicherung eingerichtet werden. Weitere Informationen über Sicherheitseinstellungen und Überwachungsrichtlinien finden Sie in der Windows-Dokumentation.

Windows-Benachrichtigungen

Für den Fall, dass ein System- oder Benutzerproblem auftritt, konfigurieren Sie das Netzwerk so, dass es eine automatische Nachricht an eine bestimmte Person, z. B. den Systemadministrator, auf dem gleichen oder einem anderen Computer sendet.

- Starten Sie auf dem versendenden wie auch auf dem empfangenden Computer den Benachrichtigungsdienst unter „Services“ in der Windows-Systemsteuerung.
- Starten Sie auf dem versendenden Computer den Benachrichtigungsdienst unter „Services“ (Dienste) in der Windows-Systemsteuerung.

Weitere Informationen über das Erstellen eines Benachrichtigungsobjekts finden Sie in der Windows-Dokumentation.

Elektronische Lizenzierung 3

Bei SCIEX OS kann die elektronische Lizenzierung knotengebunden oder serverbasiert sein. Bei der Central Administrator Console (CAC) Software kann die elektronische Lizenzierung nur knotengebunden sein.

Die Aktivierungs-ID wird möglicherweise für zukünftigen Service oder im Fall von Supportanfragen benötigt. Zugriff auf die Aktivierungs-ID einer knoten- oder serverbasierten Lizenz:

- Klicken Sie im Arbeitsbereich „Configuration“ im SCIEX OS-Fenster auf **Licenses**.

Hinweis: Stellen Sie sicher, dass Sie die Lizenz verlängern, bevor sie abläuft.

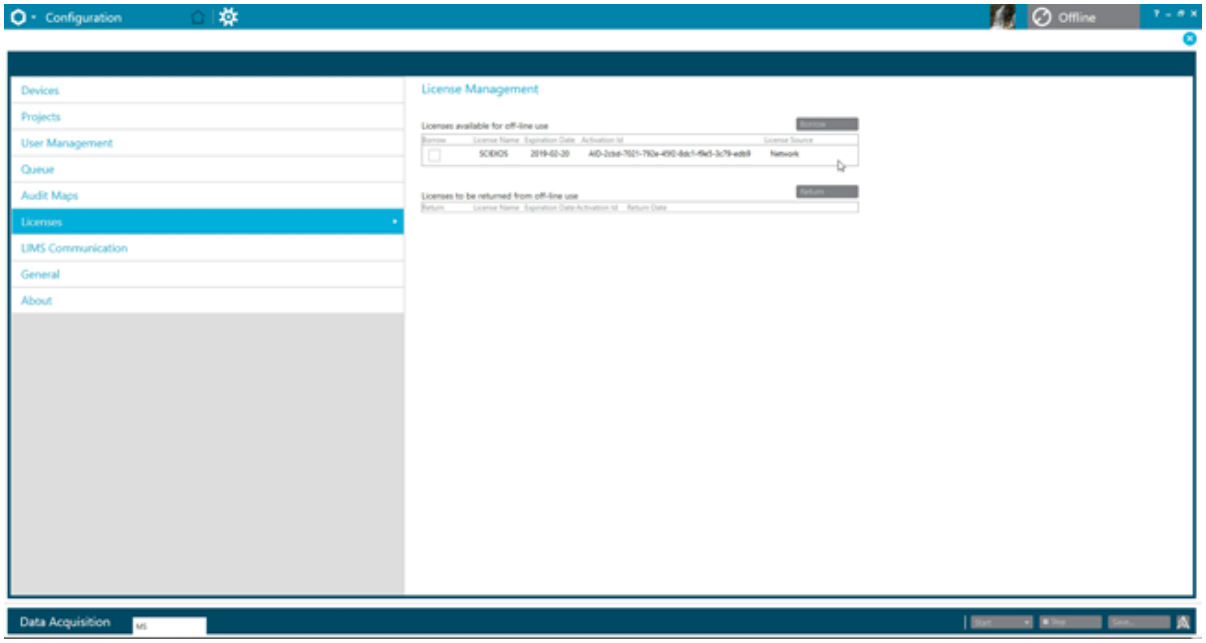
Ausleihen einer serverbasierten elektronischen Lizenz

Für die Verwendung von SCIEX OS ist eine Lizenz erforderlich. Wenn die serverbasierte Lizenzierung zum Einsatz kommt, können Benutzer, die offline arbeiten möchten, für die Dauer von bis zu 7 Tagen eine Lizenz reservieren. Während dieser Zeit ist die ausgeliehene elektronische Lizenz für den Computer reserviert.

Hinweis: Dieses Verfahren gilt nicht für die Central Administrator Console (CAC) Software.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Licenses**.
   Die Tabelle „Licenses available for off-line use“ zeigt alle für das Ausleihen verfügbare Lizenzen an.

Abbildung 3-1: Lizenzmanagement: Ausleihen einer Lizenz



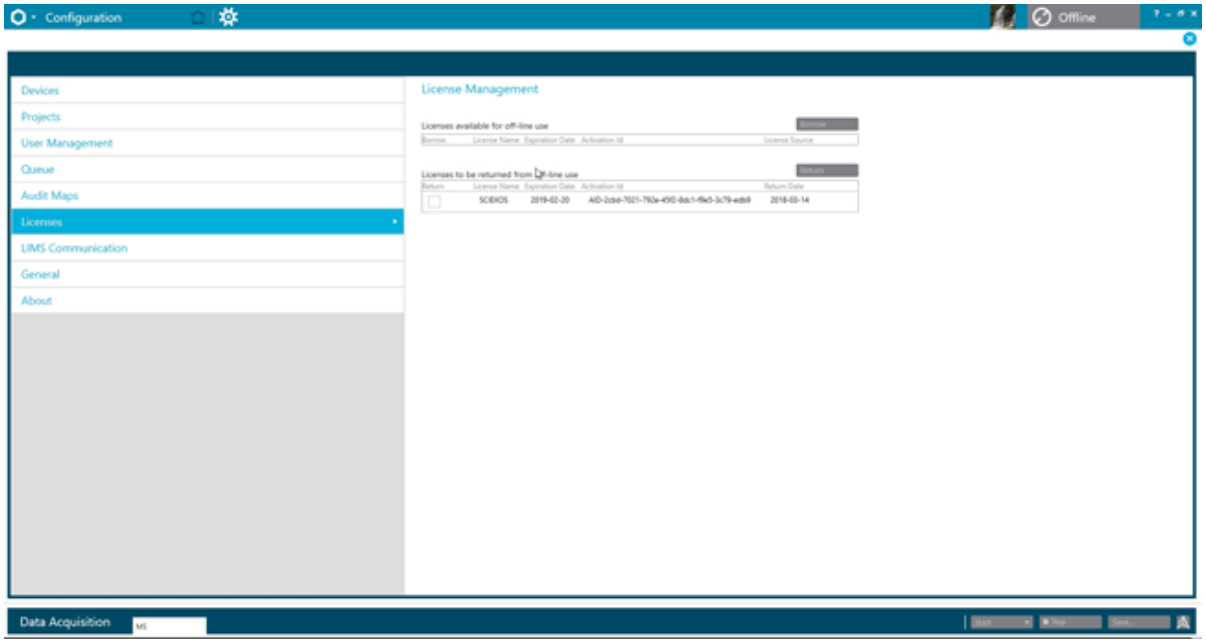
3. Wählen Sie die auszuleihende Lizenz aus und klicken Sie dann auf **Borrow**.

Zurückgeben einer serverbasierten elektronischen Lizenz

Hinweis: Dieses Verfahren gilt nicht für die Central Administrator Console (CAC) Software.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Licenses**.
   Die Tabelle „Licenses to be returned from off-line use“ zeigt alle Lizenzen, die zurückgegeben werden können, d. h. alle Lizenzen, die von diesem Computer ausgeliehen wurden.

Abbildung 3-2: Lizenzmanagement: Zurückgeben einer Lizenz



3. Wählen Sie die zurückzugebende Lizenz aus und klicken Sie dann auf **Return**.

Zugriffssteuerung 4

In diesem Abschnitt wird die Steuerung des Zugriffs auf SCIEX OS beschrieben. Um den Zugriff auf SCIEX OS zu steuern, führt der Administrator die folgenden Aufgaben aus:

Hinweis: Um die Aufgaben in diesem Abschnitt ausführen zu können, muss der Benutzer über lokale Administratorrechte für die Workstation verfügen, auf der die Software installiert wird.

- Installation und Konfiguration von SCIEX OS
- Hinzufügen und Konfigurieren von Benutzern und Rollen
- Konfiguration des Zugriffs auf die Projekte und Projektdateien im Stammverzeichnis

Dieses Verfahren bietet Anweisungen für die lokale Verwaltung von SCIEX OS. Informationen über die zentrale Verwaltung von SCIEX OS finden Sie im Abschnitt: Central Administrator Console

Hinweis: Änderungen der SCIEX OS-Konfiguration werden nach dem Neustart von SCIEX OS wirksam.

Speicherplatz der sicherheitsrelevanten Informationen

Alle Sicherheitsinformationen werden auf dem lokalen Computer im Ordner `C:\ProgramData\SCIEX\Clearcore2.Acquisition` in einer Datei namens `Security.data` gespeichert.

Workflow für die Software-Sicherheit

SCIEX OS arbeitet mit den Sicherheits-, Anwendungs- und System-Ereignisüberwachungs-Komponenten der Windows Administrative Tools zusammen.

Die Sicherheit muss auf den folgenden Ebenen konfiguriert werden:

- Windows-Authentifizierung: Zugriff auf den Computer.
- Windows-Autorisierung: Zugriff auf Dateien und Ordner.
- SCIEX OS-Authentifizierung: Die Möglichkeit, SCIEX OS zu öffnen.
- SCIEX OS-Autorisierung: Zugriff auf die Funktionen in SCIEX OS.

Für eine Liste der Aufgaben im Rahmen der Sicherheitskonfiguration siehe die Tabelle: Tabelle 4-1. Für Optionen bei der Einstellung der verschiedenen Sicherheitsebenen siehe die Tabelle: Tabelle 4-2.

Tabelle 4-1: Workflow zum Konfigurieren der Sicherheit

Aufgabe	Verfahren
Installation von SCIEX OS.	Siehe das Dokument: *SCIEX OS Software-Installationshandbuch*.
Konfiguration des Zugriffs auf SCIEX OS	Siehe Abschnitt: Konfiguration des Zugriffs auf SCIEX OS.
Konfiguration der Windows-Dateisicherheit und NTFS	Siehe Abschnitt: Konfigurieren des Zugriffs auf Projekte und Projektdateien.

Tabelle 4-2: Optionen bei der Sicherheitskonfiguration

Option	CFR 21 Teil 11
Windows-Sicherheit	
Konfiguration von Benutzern und Gruppen (Authentifizierung)	Ja
Aktivierung der Windows-Überwachung sowie der Datei- und Verzeichnisüberwachung	Ja
Einstellung von Dateiberechtigungen (Autorisierung)	Ja
SCIEX OS-Installation	
Installation von SCIEX OS.	Ja
Öffnen des Event Viewers zur Installationsprüfung	Ja
Software-Sicherheit	
Auswählen des Sicherheitsmodus	Ja
Konfigurieren der Benutzer und Rollen von SCIEX OS	Ja
Konfiguration von E-Mail-Benachrichtigungen	Ja
Erstellen von Audit-Map-Vorlagen, Konfigurieren von Audit-Trail-Maps für Projekte und Workstations	Ja
Aktivieren der Prüfsummen-Funktion für wiff-Dateien	Ja
Allgemeine Aufgaben	
Hinzufügen neuer Projekte	Ja

Installation von SCIEX OS

Lesen Sie vor der Installation von SCIEX OS diese Dokumente, die auf der Softwareinstallations-DVD oder im Web-Download-Paket verfügbar sind: *Software-Installationshandbuch* und *Versionshinweise*. Stellen Sie sicher, dass Sie den Unterschied zwischen einem Verarbeitungscomputer und einem Erfassungscomputer kennen. Führen Sie dann die entsprechende Installation durch.

Systemvoraussetzungen

Angaben zu den Mindestanforderungen für die Installation finden Sie im Dokument: *Software-Installationshandbuch*.

Voreingestellte Auditing-Optionen

Für eine Beschreibung der installierten Audit-Maps siehe Abschnitt: Installierte Audit-Map-Vorlagen. Nach der Installation kann der SCIEX OS-Administrator benutzerdefinierte Audit Maps erstellen und im Arbeitsbereich „Configuration“ eine andere Audit Map zuweisen.

Konfigurieren des Sicherheitsmodus

In diesem Abschnitt werden die Optionen des „Security Mode“ beschrieben, die auf der Seite „User Management“ im Arbeitsbereich „Configuration“ enthalten sind.

Integrated Mode: Wenn der aktuell unter Windows angemeldete Benutzer als Benutzer in der Software definiert ist, dann hat dieser Benutzer Zugriff auf SCIEX OS.

Integrated Mode: Wenn der aktuell unter Windows angemeldete Benutzer als Benutzer in der Software definiert ist, dann hat dieser Benutzer Zugriff auf die Software.

Mixed Mode: Benutzer melden sich bei Windows und der Software separat an. Die für die Anmeldung bei Windows verwendeten Anmeldedaten müssen nicht mit den Anmeldedaten für übereinstimmen. Verwenden Sie diesen Modus, um einer Benutzergruppe die Anmeldung bei Windows mit den gleichen Anmeldeinformationen zu ermöglichen. Für die Anmeldung bei der Software benötigt jeder Benutzer jedoch eindeutige Anmeldedaten. Diesen eindeutigen Anmeldedaten können bestimmte Rollen in der gleichen Art und Weise wie im „Integrated Mode“ zugewiesen werden.

Wenn der „Mixed Mode“ ausgewählt ist, stehen die Funktionen „Screen Lock“ und „Auto Logoff“ zur Verfügung.

Screen Lock and Auto Logoff: Aus Sicherheitsgründen kann der Computerbildschirm nach Ablauf einer bestimmten Zeit der Inaktivität gesperrt werden. Es kann zudem ein automatischer Logoff-Timer definiert werden, sodass die Software geschlossen wird, nachdem sie eine bestimmte Zeit gesperrt war. „Screen Lock“ und „Auto Logoff“ sind nur im „Mixed Mode“ verfügbar.

Hinweis: Wenn der Bildschirm gesperrt wird, werden die Erfassung und Verarbeitung fortgesetzt. Eine automatische Abmeldung erfolgt nicht, wenn die Verarbeitung erfolgt oder die „Results Table“ nicht gespeichert wurde. Wenn der Benutzer mit einer erzwungenen Abmeldung abgemeldet wird, dann werden alle Verarbeitungsvorgänge gestoppt und nicht gespeicherte Daten gehen verloren. Die Erfassung wird fortgesetzt, nachdem der Benutzer automatisch oder manuell abgemeldet wurde.

Security Notification: Die Software kann so konfiguriert werden, dass eine E-Mail-Benachrichtigung nach einer konfigurierbaren Anzahl von Anmeldefehlern innerhalb eines definierbaren Zeitraums automatisch gesendet wird, um vor Zugriffen auf das System durch nicht autorisierte Benutzer zu warnen. Die Anzahl der Anmeldefehler kann zwischen 3 und 7 betragen und der Zeitraum zwischen 5 Minuten und 24 Stunden.

Hinweis: Für Arbeitsgruppen, die mithilfe der Central Administrator Console (CAC)-Software verwaltet werden, kann der Sicherheitsmodus nicht mit SCIEX OS verwaltet werden.

Auswählen des Sicherheitsmodus

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **User Management**.
3. Klicken Sie auf die Registerkarte **Security Mode**.
4. Wählen Sie **Integrated Mode** oder **Mixed Mode** aus. Siehe Abschnitt: Konfigurieren des Sicherheitsmodus.
5. Klicken Sie auf **Save**.
   Ein Bestätigungsdialogfeld wird angezeigt.
6. Klicken Sie auf **OK**.

Konfigurieren der Workstation-Sicherheitsoptionen (Mixed Mode)

Voraussetzungen
• Stellen Sie den Sicherheitsmodus auf „Mixed Mode“ ein. Siehe Abschnitt: Konfigurieren des Sicherheitsmodus.

Wenn der „Mixed Mode“ ausgewählt ist, dann können die Funktionen „Screen Lock“ und „Auto Logoff“ konfiguriert werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **User Management**.
3. Öffnen Sie die Registerkarte „Security Mode“.
4. Um die Funktion „Screen Lock“ zu konfigurieren, gehen Sie wie folgt vor:
   a. Wählen Sie **Screen Lock** aus.
   b. Geben Sie im Feld **Wait** eine Zeit in Minuten an.
      Wenn die Workstation für diese Zeitdauer inaktiv ist, dann wird sie automatisch gesperrt. Der angemeldete Benutzer kann die Workstation entsperren, indem er die korrekten Anmeldedaten eingibt, oder der Administrator kann den Benutzer abmelden.
5. Um die Funktion „Auto Logoff“ zu konfigurieren, gehen Sie wie folgt vor:
   a. Wählen Sie **Auto Logoff** aus.
   b. Geben Sie im Feld **Wait** eine Zeit in Minuten an. Wenn die Workstation für diese Zeitdauer automatisch oder manuell gesperrt wird, dann wird der aktuell angemeldete Benutzer abgemeldet. Alle Verarbeitungsvorgänge werden gestoppt. Die Erfassung wird jedoch fortgesetzt.

6. Klicken Sie auf **Save**.
   Ein Bestätigungsdialogfeld wird geöffnet.
7. Klicken Sie auf **OK**.

Konfigurieren der E-Mail-Benachrichtigung (Mixed Mode)

Voraussetzungen
• Stellen Sie den Sicherheitsmodus auf „Mixed Mode“ ein. Siehe Abschnitt: Konfigurieren des Sicherheitsmodus.

Die Software kann so konfiguriert werden, dass eine E-Mail-Nachricht nach einer konfigurierbaren Anzahl von Anmeldefehlern innerhalb eines definierbaren Zeitraums gesendet wird. Die Anzahl der Anmeldefehler kann zwischen 3 und 7 betragen und der Zeitraum zwischen 5 Minuten und 24 Stunden.

Der Computer, auf dem die Software installiert ist, muss mit einem SMTP-Server mit offenem Port kommunizieren können.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **User Management**.
3. Öffnen Sie die Registerkarte „Security Mode“.
4. Aktivieren Sie das Kontrollkästchen **Send e-mail messages after** und geben Sie dann an, wie viele Anmeldefehler innerhalb welchen Zeitraums (in Minuten) eine E-Mail-Benachrichtigung generieren sollen.

   Tipp! Um die Benachrichtigung zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Send e-mail messages after**.
5. Im Feld **SMTP Server** geben Sie den Namen des SMTP-Servers ein.

   Hinweis: Das SMTP-Konto sendet Mails an den E-Mail-Server. Der SMTP-Server ist in der E-Mail-Anwendung des Unternehmens definiert.
6. Geben Sie im Feld **Port Number** die Nummer des offenen Ports ein.
   Klicken Sie auf **Apply Default**, um die Standard-Port-Nummer 25 einzufügen.
7. Geben Sie im Feld **To** die E-Mail-Adresse ein, an die die Nachricht gesendet werden soll. Beispiel: username@domain.com.
8. Geben Sie im Feld **From** die E-Mail-Adresse ein, die im Feld **From** der Nachricht angezeigt werden soll.
9. Im Feld **Subject** geben Sie den Betreff der Nachricht ein.
10. Geben Sie im Feld **Message** den Text ein, der im Nachrichtentext enthalten sein soll.
11. Klicken Sie auf **Save**.
    Ein Bestätigungsdialogfeld wird geöffnet.
12. Klicken Sie auf **OK**.

13. Um die Konfiguration zu überprüfen, klicken Sie auf **Send Test Mail**.

Konfiguration des Zugriffs auf SCIEX OS

Gehen Sie folgendermaßen vor, bevor Sie die Sicherheit konfigurieren:

- Entfernen Sie alle unnötigen Benutzer und Benutzergruppen, wie z. B. „Replicator“, „Power User“ und „Backup Operator“, vom lokalen Computer und vom Netzwerk.

  Hinweis: Jeder SCIEX-Computer ist mit einem lokalen Konto auf Administratorebene konfiguriert, **abservice**. Dieses Konto wird vom SCIEX-Dienst und dem technischen Support für das Installieren, Warten und Unterstützen des Systems verwendet. Dieses Konto darf nicht gelöscht oder deaktiviert werden. Wenn das Konto gelöscht oder deaktiviert werden muss, dann entwickeln Sie einen alternativen Plan für den SCIEX-Zugriff und teilen Sie dies dem zuständigen Außendienstmitarbeiter mit.

- Fügen Sie Benutzergruppen hinzu, die Gruppen ohne administrative Aufgaben enthalten.
- Konfigurieren Sie die Systemberechtigungen.
- Erstellen Sie anhand von Gruppenrichtlinien geeignete Verfahren und Kontenrichtlinien für die Benutzer.

In der Windows-Dokumentation finden Sie weitere Informationen zu folgenden Themen:

- Benutzer und Gruppen und Active-Directory-Benutzer
- Passwort und Kontosperrrichtlinien für Benutzerkonten
- Richtlinien zu Benutzerrechten

Wenn Benutzer in einer „Active Directory“-Umgebung arbeiten, wirken sich die Einstellungen der „Active Directory“-Gruppenrichtlinien auf die Computer-Sicherheit aus. Besprechen Sie im Rahmen einer umfassenden SCIEX OS-Bereitstellung die Gruppenrichtlinien mit Ihrem Active-Directory-Administrator.

SCIEX OS Berechtigungen

Abbildung 4-1: Seite „User Management“

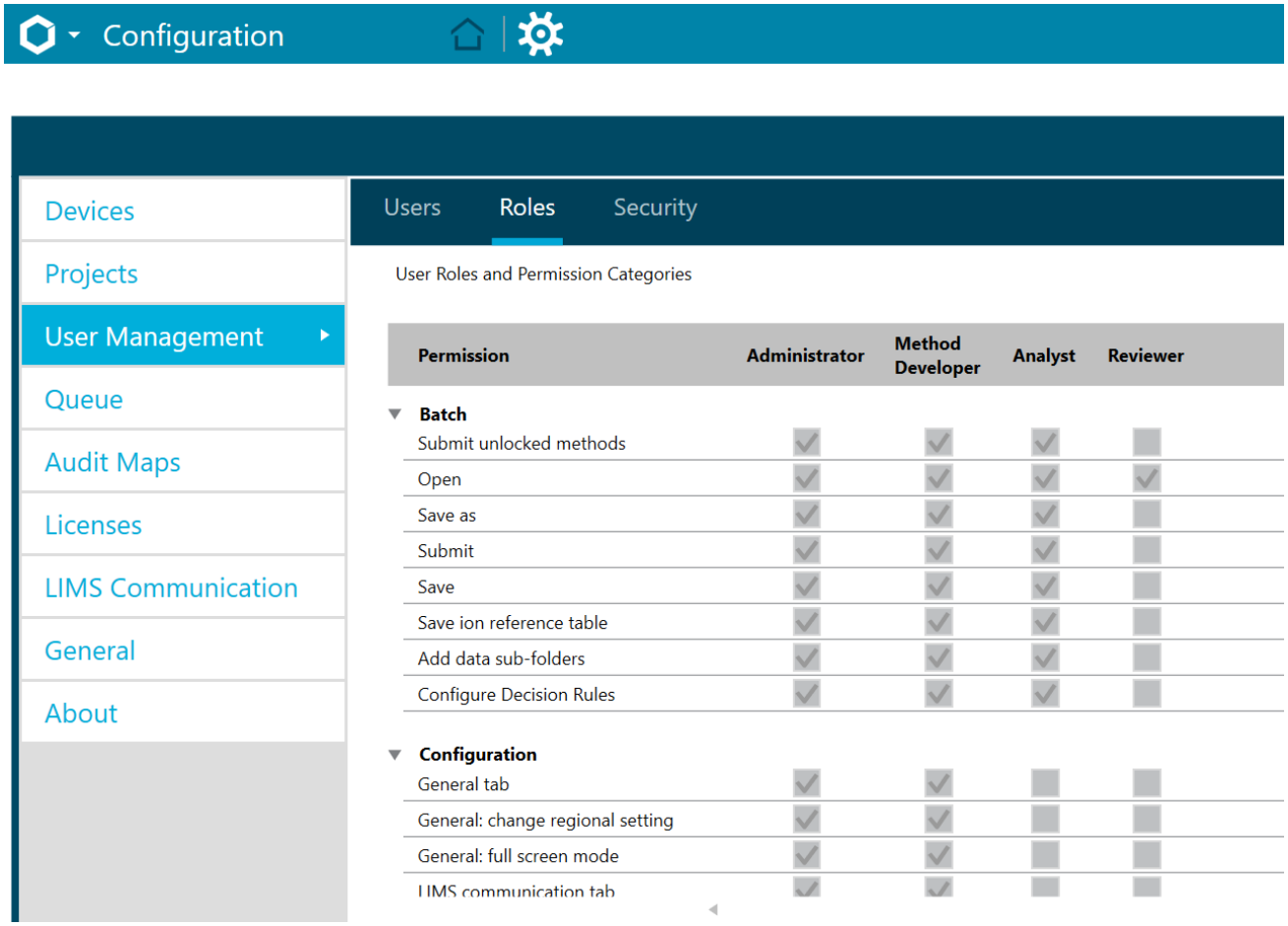


Tabelle 4-3: Berechtigungen

Berechtigung	Beschreibung
Batch (Charge)	
Submit unlocked methods	(Entsperrte Methoden übergeben) Erlaubt den Benutzern das Übergeben von Chargen, die entsperrte Methoden enthalten.
Open	(Öffnen) Erlaubt den Benutzern das Öffnen bestehender Chargen.
Save as	(Speichern unter) Erlaubt den Benutzern das Speichern von Chargen unter einem neuen Namen.
Submit	(Übergeben) Erlaubt den Benutzern das Übergeben von Chargen.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Save	(Speichern) Erlaubt den Benutzern das Speichern einer Charge, wobei die vorhandenen Inhalte überschrieben werden.
Save ion reference table	(Ionenreferenztabelle speichern) Erlaubt den Benutzern die Bearbeitung der Ionenreferenztabelle.
Add data sub-folders	(Daten-Unterordner hinzufügen) Erlaubt den Benutzern die Erstellung von Unterordnern für das Speichern von Daten.
Configure Decision Rules	(Entscheidungsregeln konfigurieren) Erlaubt den Benutzern das Hinzufügen und Ändern von Entscheidungsregeln.
Configuration (Konfiguration)	
General tab	(Registerkarte „Allgemein“) Erlaubt den Benutzern das Öffnen der Seite „General“ im Arbeitsbereich „Configuration“.
General: change regional setting	(Allgemein: Regionseinstellungen ändern) Erlaubt den Benutzern die Übernahme der aktuellen regionalen Einstellungen des Systems in SCIEX OS.
General: full screen mode	(Allgemein: Vollbildmodus) Erlaubt den Benutzern die Aktivierung bzw. Deaktivierung des Vollbildmodus.
General: Stop Windows services	(Allgemein: Windows Services stoppen) Erlaubt es den Benutzern die Option **Windows Settings** zu aktivieren oder zu deaktivieren.
LIMS communication tab	(Registerkarte „LIMS-Kommunikation“) Erlaubt den Benutzern das Öffnen der Seite „LIMS Communication“ im Arbeitsbereich „Configuration“.
Audit maps tab	(Registerkarte „Audit-Maps“) Erlaubt den Benutzern das Öffnen der Seite „Audit Maps“ im Arbeitsbereich „Configuration“.
Queue tab	(Registerkarte „Warteschlange“) Erlaubt den Benutzern das Öffnen der Seite „Queue“ im Arbeitsbereich „Configuration“.
Queue: instrument idle time	(Warteschlange: Geräteleerlaufzeit) Erlaubt den Benutzern die Einstellung der Geräteleerlaufzeit.
Queue: max number of acquired samples	(Warteschlange: Maximale Anzahl erfasster Proben) Erlaubt den Benutzern die Einstellung der maximal zulässigen Anzahl an erfassten Proben.
Queue: other queue settings	(Warteschlange: Andere Warteschlangeneinstellungen) Erlaubt den Benutzern die Konfiguration anderer Warteschlangeneinstellungen.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Projects tab	(Registerkarte „Projekte“) Erlaubt den Benutzern das Öffnen der Seite „Projects“ im Arbeitsbereich „Configuration“.
Projects: create project	(Projekte: Projekt erstellen) Erlaubt den Benutzern das Erstellen von Projekten.
Projects: apply an audit map template to an existing project	(Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden) Erlaubt den Benutzern die Anwendung einer Audit-Map auf ein Projekt.
Projects: create root directory	(Projekte: Stammverzeichnis erstellen) Erlaubt den Benutzern die Erstellung eines Stammverzeichnisses für das Speichern von Projekten.
Projects: set current root directory	(Projekte: Aktuelles Stammverzeichnis festlegen) Erlaubt den Benutzern das Ändern des Stammverzeichnisses für ein Projekt.
Projects: specify network credentials	(Projekte: Netzwerkanmeldedaten festlegen) Erlaubt den Benutzern das Festlegen eines sicheren Netzwerkkontos (SNA), das während der Netzwerkerfassung verwendet wird, wenn der angemeldete Benutzer keinen Zugriff auf die Netzwerkressource hat.
Projects: Enable checksum writing for wiff data creation	(Projekte: Schreiben der Prüfsumme für die wiff-Datenerstellung aktivieren) Erlaubt den Benutzern das Konfigurieren der Software, um Prüfsummen in wiff-Datendateien zu schreiben.
Projects: clear root directory	(Projekte: Stammverzeichnis löschen) Benutzer können ein Stammverzeichnis aus der Liste löschen.
Devices tab	(Registerkarte „Geräte“) Erlaubt den Benutzern das Öffnen der Seite „Devices“ im Arbeitsbereich „Configuration“.
User management tab	(Registerkarte „Benutzerverwaltung“) Erlaubt den Benutzern das Öffnen der Seite „User Management“ im Arbeitsbereich „Configuration“.
Force user logoff	(Abmeldung des Benutzers erzwingen) Erlaubt den Benutzern, die Abmeldung eines aktuell bei SCIEX OS angemeldeten Benutzers zu erzwingen. Erlaubt den Benutzern, die Abmeldung eines aktuell bei der SCIEX OS Software angemeldeten Benutzers zu erzwingen.
Event Log (Ereignisprotokoll)	
Access event log workspace	(Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen) Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Event Log“.
Archive log	(Ereignisprotokoll archivieren) Erlaubt den Benutzern das Archivieren des Ereignisprotokolls.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Audit Trail (Audit-Trail)	
Access audit trail workspace	(Auf Arbeitsbereich „Audit-Trail“ zugreifen) Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Audit Trail“.
View active audit map	(Aktive Audit-Map anzeigen) Erlaubt den Benutzern das Anzeigen der aktiven Audit-Map für eine Workstation oder ein Projekt im Arbeitsbereich „Audit Trail“.
Print/Export audit trail	(Audit-Trail drucken/exportieren) Erlaubt den Benutzern das Drucken oder Exportieren des Audit-Trails.
CAC Server (CAC-Server) (nur CAC)	
Manage Workgroups	(Arbeitsgruppen verwalten) Erlaubt den Benutzern das Erstellen und Verwalten von Arbeitsgruppen im Arbeitsbereich „User Management“.
Manage Workgroups Projects	(Arbeitsgruppen-Projekte verwalten) Erlaubt den Benutzern das Erstellen und Verwalten von Arbeitsgruppen-Projekten im Arbeitsbereich „User Management“.
Data Acquisition Panel (Teilfenster „Datenerfassung“)	
Start	(Starten) Erlaubt den Benutzern das Starten der Erfassung im Teilfenster „Data Acquisition“.
Stop	(Stoppen) Erlaubt den Benutzern das Stoppen der Erfassung im Teilfenster „Data Acquisition“.
Save	(Speichern) Erlaubt den Benutzern das Speichern von erfassten Daten mit einem anderen Dateinamen im Teilfenster „Data Acquisition“.
MS & LC Method (MS & LC Methode)	
Access method workspace	(Auf Arbeitsbereich „Methode“ zugreifen) Erlaubt den Benutzern das Öffnen der Arbeitsbereiche „MS Method“ und „LC Method“.
New	(Neu) Erlaubt den Benutzern die Erstellung von MS- und LC-Methoden.
Open	(Öffnen) Erlaubt den Benutzern das Öffnen von MS- und LC-Methoden.
Save	(Speichern) Erlaubt den Benutzern das Speichern einer Methode, wobei bestehende Inhalte überschrieben werden.
Save as	(Speichern unter) Erlaubt den Benutzern das Speichern von Methoden unter einem neuen Namen.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Lock/Unlock method	(Methode sperren/entsperren) Erlaubt den Benutzern das Sperren von Methoden, um deren Bearbeitung zu verhindern, sowie das Entsperren von Methoden.
Queue (Warteschlange)	
Manage	(Verwalten) Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Queue“.
Start/Stop	(Start/Stopp) Erlaubt den Benutzern das Starten und Stoppen der Warteschlange.
Print	(Drucken) Erlaubt den Benutzern das Drucken der Warteschlange.
Library (Bibliothek)	
Access library workspace	(Auf Arbeitsbereich „Bibliothek“ zugreifen) Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Library“. Gilt nicht für den Quantifizierungs-Workflow.
CAC settings (CAC Client)	
Enable Central Administration	(Zentraladministration aktivieren) Erlaubt den Benutzern das Konfigurieren von SCIEX OS für die Zentraladministration mit der Central Administrator Console (CAC) Software.
MS Tune (MS Tune)	
Access MS Tune workspace	(Auf Arbeitsbereich „MS Tune“ zugreifen) Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „MS Tune“.
Advanced MS tuning	(Erweitertes MS-Tuning) (X500 QTOF-Systeme) Erlaubt den Benutzern den Zugriff auf erweiterte Tuning-Optionen, wie beispielsweise „Detector Optimization“, „Positive and Negative Q1 Unit Tuning“, „Positive and Negative TOF MS Tuning“ und „Positive and Negative Q1 High Tuning“.
Advanced troubleshooting	(Erweiterte Fehlerbehebung) Erlaubt den Benutzern das Öffnen des Dialogfeldes „Advanced Troubleshooting“.
Quick status check	(Schnelle Statusüberprüfung) (X500 QTOF-Systeme) Erlaubt den Benutzern die Durchführung schneller positiver und negativer Statusüberprüfungen.
Restore instrument data	(Gerätedaten wiederherstellen) Erlaubt den Benutzern die Wiederherstellung zuvor gespeicherter Tuning-Einstellungen.
Explorer (Explorer)	
Access Explorer workspace	(Auf Arbeitsbereich „Explorer“ zugreifen) Erlaubt den Benutzern das Öffnen des Arbeitsbereichs „Explorer“.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Export	(Exportieren) Erlaubt den Benutzern das Exportieren von Daten aus dem Arbeitsbereich „Explorer“.
Print	(Drucken) Erlaubt den Benutzern das Drucken von Daten im Arbeitsbereich „Explorer“.
Options	(Optionen) Erlaubt den Benutzern das Ändern der Optionen für den Arbeitsbereich „Explorer“.
Recalibrate	(Rekalibrieren) Erlaubt den Benutzern das erneute Kalibrieren von Proben und Spektren im Arbeitsbereich „Explorer“. Gilt nicht für den Quantifizierungs-Workflow.
Analytics (Analyse)	
New results	(Neue Ergebnisse) Erlaubt den Benutzern die Erstellung von „Results Tables“.
Create processing method	(Verarbeitungsmethode erstellen) Erlaubt den Benutzern die Erstellung von Verarbeitungsmethoden.
Modify processing method	(Verarbeitungsmethode ändern) Erlaubt den Benutzern das Ändern von Verarbeitungsmethoden.
Allow Export and Create Report of unlocked Results Table	(Export nicht gesperrter „Results Table“ und Erstellen eines Berichts aus dieser erlauben) Erlaubt den Benutzern, eine nicht gesperrte „Results Table“ oder Statistiktabelle zu exportieren und einen Bericht aus dieser zu erstellen.
Save results for Automation Batch	(Ergebnisse für Automatisierungs-Charge speichern) Ermöglicht das Speichern von „Results Tables“, die im Arbeitsbereich „Batch“ automatisch erstellt wurden. Diese Berechtigung ist für die automatische Verarbeitung während der Erfassung erforderlich.
Change default quantitation method integration algorithm	(Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern) Erlaubt den Benutzern das Ändern des Integrationsalgorithmus in den Standardeinstellungen des Projekts.
Change default quantitation method integration parameters	(Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern) Erlaubt den Benutzern das Ändern der Integrationsparameter in den Standardeinstellungen des Projekts.
Enable project modified peak warning	(Warnung bei veränderten Peaks eines Projekt aktivieren) Erlaubt den Benutzern die Freigabe von Warnungen bei geänderten Peaks für ein Projekt.
Add samples	(Proben hinzufügen) Erlaubt den Benutzern das Hinzufügen von Proben zu einer „Results Table“.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Remove selected samples	(Ausgewählte Proben entfernen) Erlaubt den Benutzern das Entfernen von Proben aus einer „Results Table“.
Export, import, or remove external calibration	(Externe Kalibrierung exportieren, importieren oder entfernen) Erlaubt den Benutzern das Exportieren, Importieren oder Entfernen von externen Kalibrierungen.
Modify sample name	(Probenname ändern) Erlaubt den Benutzern das Ändern des Probennamens in der „Results Table“.
Modify sample type	(Probentyp ändern) Erlaubt den Benutzern das Ändern des Probentyps, wie beispielsweise „Standard“, „Quality control (QC)“ oder „Unknown“ in der „Results Table“.
Modify sample ID	(Proben-ID ändern) Erlaubt den Benutzern das Ändern der Proben-ID in der „Results Table“.
Modify actual concentration	(Istkonzentration ändern) Erlaubt den Benutzern das Ändern der Istkonzentration der Standard- und QC-Proben in der „Results Table“.
Modify dilution factor	(Verdünnungsfaktor ändern) Erlaubt den Benutzern das Ändern des Verdünnungsfaktors in der „Results Table“.
Modify comment fields	(Kommentarfelder ändern) Erlaubt den Benutzern das Ändern der Kommentarfelder: • Component Comment • IS Comment • IS Peak Comment • Peak Comment • Sample Comment
Enable manual integration	(Manuelle Integration aktivieren) Erlaubt den Benutzern die Durchführung einer manuellen Integration.
Set peak to Not Found	(Peak auf „nicht gefunden“ setzen) Erlaubt den Benutzern das Setzen eines Peaks auf „**Not Found**“.
Include or exclude a peak from the Results Table	(Einen Peak in die „Results Table“ aufnehmen oder ausschließen) Erlaubt es den Benutzern, Peaks in die „Results Table“ einzubeziehen oder aus ihr auszuschließen.
Regression options	(Regressionsoptionen) Erlaubt den Benutzern das Ändern der Regressionsoptionen im Bereich „Calibration Curve“.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Modify Results Table integration parameters for a single chromatogram	(Integrationsparameter für ein Einzelchromatogramm in der Ergebnistabelle ändern) Erlaubt den Benutzern das Ändern der Integrationsparameter für ein Einzelchromatogramm im Bereich „Peak Review“.
Modify quantitation method for the Results Table component	(Quantifizierungsmethode für Komponente der „Results Table“ modifizieren) Erlaubt den Benutzern die Auswahl einer anderen Verarbeitungsmethode für eine Komponente im Bereich „Peak Review“ mit der Option **Update Processing Method for Component**.
Create metric plot new settings	(Neue Einstellungen für metrische Darstellungen erstellen) Erlaubt den Benutzern die Erstellung neuer metrischer Darstellungen sowie die Änderung der Einstellungen.
Add custom columns	(Benutzerdefinierte Spalten hinzufügen) Erlaubt den Benutzern das Hinzufügen von benutzerdefinierten Spalten zu einer „Results Table“.
Set peak review title format	(Titelformat für die Peak-Überprüfung festlegen) Erlaubt den Benutzern das Ändern des Titels der Peak-Prüfung.
Remove custom column	(Benutzerdefinierte Spalte entfernen) Erlaubt den Benutzern das Entfernen von benutzerdefinierten Spalten aus einer „Results Table“.
Results Table display settings	(Einstellungen für die Anzeige der „Results Table“) Erlaubt den Benutzern die benutzerdefinierte Anpassung der Spalten, die in der „Results Table“ angezeigt werden.
Lock Results Table	(„Results Table“ sperren) Erlaubt den Benutzern das Sperren einer „Results Table“, um deren Bearbeitung zu verhindern.
Unlock Results Table	(„Results Table“ entsperren) Erlaubt den Benutzern das Entsperren einer „Results Table“, um deren Bearbeitung zu ermöglichen.
Mark Results file as reviewed and save	(Ergebnisdatei als „geprüft“ kennzeichnen und speichern) Erlaubt den Benutzern die Kennzeichnung einer „Results Table“ als „geprüft“ sowie deren Speicherung.
Modify report template	(Berichtsvorlage ändern) Erlaubt den Benutzern das Ändern von Berichtsvorlagen.
Transfer results to LIMS	(Ergebnisse in LIMS übertragen) Erlaubt den Benutzer den Upload von Ergebnissen in ein Laboratory Information Management System (LIMS).
Modify barcode column	(Spalte „Barcode“ ändern) Erlaubt den Benutzern das Ändern der Spalte „**Barcode**“ in einer „Results Table“.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Change comparison sample assignment	(Zuweisung der Vergleichsprobe ändern) Erlaubt den Benutzern das Ändern der Vergleichsprobe, die in der Spalte „**Comparison**“ der „Results Table“ angegeben ist.
Add the MSMS spectra to library	(MSMS-Spektren der Bibliothek hinzufügen) Erlaubt den Benutzern das Hinzufügen der ausgewählten MS/MS-Spektren zu einer Bibliothek. Gilt nicht für den Quantifizierungs-Workflow.
Project default settings	(Standardmäßige Projekteinstellungen) Erlaubt den Benutzern das Ändern der Standardeinstellungen des Projekts für die quantitative und qualitative Verarbeitung.
Create report in all formats	(Bericht in allen Formaten erstellen) Erlaubt den Benutzern, Berichte in allen Formaten zu generieren. Benutzer ohne Berechtigung können Berichte nur im PDF-Format generieren.
Edit flagging criteria parameters	(Parameter für die Markierungskriterien bearbeiten) Erlaubt den Benutzern das Ändern der Parameter für die Markierung in einer Verarbeitungsmethode.
Automatic outlier removal parameter change	(Parameter für das automatische Entfernen von Ausreißern ändern) Erlaubt den Benutzern das Ändern der Parameter für das automatische Entfernen von Ausreißern.
Enable automatic outlier removal	(Automatische Entfernung von Ausreißern aktivieren) Erlaubt den Benutzern das Ändern der Verarbeitungsmethode, um das automatische Entfernen von Ausreißern zu aktivieren.
Update processing method via FF/LS	(Verarbeitungsmethode über FF/LS aktualisieren) Erlaubt den Benutzern die Aktualisierung der Verarbeitungsmethoden mit „Formula Finder“ und „Library Search“. Gilt nicht für den Quantifizierungs-Workflow.
Update results via FF/LS	(Ergebnisse über FF/LS aktualisieren) Erlaubt den Benutzern die Aktualisierung der Ergebnisse mit „Formula Finder“ und „Library Search“. Gilt nicht für den Quantifizierungs-Workflow.
Enable grouping by adducts functionality	(Funktion der Gruppierung nach Addukten aktivieren) Erlaubt den Benutzern die Aktualisierung der Verarbeitungsmethode, um die Funktion der Gruppierung von Addukten zu aktiveren.
Browse for files	(Dateien suchen) Erlaubt den Benutzern das Suchen außerhalb des lokalen Datenordners.

Tabelle 4-3: Berechtigungen (Fortsetzung)

Berechtigung	Beschreibung
Enable standard addition	(Standard-Addition aktivieren) Erlaubt den Benutzern die Aktualisierung der Verarbeitungsmethode, um die Funktion „Standard Addition“ zu aktivieren.
Set Manual Integration Percentage Rule	(Prozentsatzregel für die manuelle Integration festlegen) Erlaubt den Benutzern die Änderung des Parameters **Manual Integration %**.

Über Benutzer und Rollen

In SCIEX OS kann der Administrator Windows-Benutzer und Gruppen zur Datenbank für die Benutzerverwaltung für SCIEX OS hinzufügen. Für den Zugriff auf die Software müssen Benutzer in der Datenbank für die Benutzerverwaltung definiert sein oder müssen ein Mitglied einer in der Datenbank definierten Gruppen sein.

Benutzer können einer oder mehreren vordefinierten Rollen, die in der folgenden Tabelle beschrieben werden, oder auch benutzerdefinierten Rollen zugewiesen werden, falls dies erforderlich ist. Die Funktionen, auf die der Benutzer zugreifen kann, werden durch Rollen festgelegt. Die vordefinierten Rollen können nicht gelöscht und ihre Berechtigungen nicht geändert werden.

Hinweis: Für Arbeitsgruppen, die mit der Central Administrator Console (CAC)-Software verwaltet werden, sind die Seiten „User Management“ schreibgeschützt.

Tabelle 4-4: Vordefinierte Rollen

Rolle	Typische Aufgaben
Administrator (Administrator)	• Verwaltet das System. • Konfiguriert die Sicherheit.
Method Developer (Methodenentwickler)	• Erstellt Methoden. • Führt Chargen aus. • Analysiert Daten zur Verwendung durch den Endbenutzer.
Analyst (Analyst)	• Führt Chargen aus. • Analysiert Daten zur Verwendung durch den Endbenutzer.
Reviewer (Prüfer)	• Prüft Daten. • Prüft Audit-Trails. • Bewertet Quantifizierungsergebnisse.

Tabelle 4-5: Voreingestellte Berechtigungen

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Batch (Charge)				
Submit unlocked methods (Entsperrte Methoden übergeben)	✓	✓	✓	×
Open (Öffnen)	✓	✓	✓	✓
Save as (Speichern unter)	✓	✓	✓	×
Submit (Übergeben)	✓	✓	✓	×
Save (Speichern)	✓	✓	✓	×
Save ion reference table (Ionenreferenztabelle speichern)	✓	✓	✓	×
Add data sub-folders (Daten-Unterordner hinzufügen)	✓	✓	✓	×
Configure Decision Rules (Entscheidungsregeln konfigurieren)	✓	✓	✓	×
Configuration (Konfiguration)				
General tab (Registerkarte „Allgemein“)	✓	✓	×	×
General: change regional setting (Allgemein: Regionseinstellungen ändern)	✓	✓	×	×
General: full screen mode (Allgemein: Vollbildmodus)	✓	✓	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
General: Stop Windows services(Allgemein: Windows Services stoppen)	✓	×	×	×
LIMS communication tab (Registerkarte „LIMS-Kommunikation“)	✓	✓	×	×
Audit maps tab (Registerkarte „Audit-Maps“)	✓	×	×	×
Queue tab (Registerkarte „Warteschlange“)	✓	✓	✓	✓
Queue: instrument idle time (Warteschlange: Geräteleerlaufzeit)	✓	✓	×	×
Queue: max number of acquired samples (Warteschlange: Maximale Anzahl erfasster Proben)	✓	✓	×	×
Queue: other queue settings (Warteschlange: Andere Warteschlangeneinstellungen)	✓	✓	×	×
Projects tab (Registerkarte „Projekte“)	✓	✓	✓	✓
Projects: create project (Projekte: Projekt erstellen)	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Projects: apply an audit map template to an existing project (Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden)	✓	×	×	×
Projects: create root directory (Projekte: Stammverzeichnis erstellen)	✓	×	×	×
Projects: set current root directory (Projekte: Aktuelles Stammverzeichnis festlegen)	✓	×	×	×
Projects: specify network credentials (Projekte: Netzwerkanmeldedaten festlegen)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Projekte: Das Schreiben der Prüfsumme für die wiff1-Datenerstellung aktivieren)	✓	×	×	×
Projects: clear root directory (Projekte: Stammverzeichnis löschen	✓	×	×	×
Devices tab (Registerkarte „Geräte“)	✓	✓	✓	×
User management tab (Registerkarte „Benutzerverwaltung“)	✓	×	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Force user logoff (Abmeldung des Benutzers erzwingen)	✓	×	×	×
Event Log (Ereignisprotokoll)				
Access event log workspace (Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen)	✓	✓	✓	✓
Archive log (Ereignisprotokoll archivieren)	✓	✓	✓	✓
Audit Trail (Audit-Trail)				
Access audit trail workspace (Auf Arbeitsbereich „Audit-Trail“ zugreifen)	✓	✓	✓	✓
View active audit map (Aktive Audit-Map anzeigen)	✓	✓	✓	✓
Print/Export audit trail (Audit-Trail drucken/exportieren)	✓	✓	✓	✓
Data Acquisition Panel (Teilfenster „Datenerfassung“)				
Start (Start)	✓	✓	✓	×
Stop (Stopp)	✓	✓	✓	×
Save (Speichern)	✓	✓	✓	×
MS & LC Method (MS & LC Methode)				
Access method workspace (Auf Arbeitsbereich „Methode“ zugreifen)	✓	✓	✓	✓
New (Neu)	✓	✓	×	×
Open (Öffnen)	✓	✓	✓	✓
Save (Speichern)	✓	✓	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Save as (Speichern unter)	✓	✓	×	×
Lock/Unlock method (Methode sperren/ entsperren)	✓	✓	×	×
Queue (Warteschlange)				
Manage (Verwalten)	✓	✓	✓	×
Start/Stop (Start/ Stopp)	✓	✓	✓	×
Print (Drucken)	✓	✓	✓	✓
Library (Bibliothek)				
Access library workspace (Auf Arbeitsbereich „Bibliothek“ zugreifen)	✓	✓	✓	✓
CAC settings (CAC Client)				
Enable Central Administration (Zentraladministration aktivieren)	✓	×	×	×
MS Tune (MS Tune)				
Access MS Tune workspace (Auf Arbeitsbereich „MS-Tune“ zugreifen)	✓	✓	✓	×
Advanced MS Tuning (Erweitertes MS-Tuning)	✓	✓	×	×
Advanced troubleshooting (Erweiterte Fehlerbehebung)	✓	✓	×	×
Quick status check (Schnelle Statusüberprüfung)	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Restore instrument data (Gerätedaten wiederherstellen)	✓	✓	×	×
Explorer (Explorer)				
Access explorer workspace (Auf Arbeitsbereich „Explorer“ zugreifen)	✓	✓	✓	✓
Export (Exportieren)	✓	✓	✓	×
Print (Drucken)	✓	✓	✓	×
Options (Optionen)	✓	✓	✓	×
Recalibrate (Rekalibrieren)	✓	✓	×	×
Analytics (Analyse)				
New results (Neue Ergebnisse)	✓	✓	✓	×
Create processing method (Verarbeitungsmethode erstellen)	✓	✓	✓	×
Modify processing method (Verarbeitungsmethode ändern)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Export nicht gesperrter „Results Table“ und Erstellen eines Berichts aus dieser erlauben)	✓	×	×	×
Save results for Automation Batch (Ergebnisse speichern für Automatisierungs-Charge)	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Change default quantitation method integration algorithm (Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern)	✓	✓	×	×
Change default quantitation method integration parameters (Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern)	✓	✓	×	×
Enable project modified peak warning (Warnung bei veränderten Peaks eines Projekts aktivieren)	✓	×	×	×
Add samples (Proben hinzufügen)	✓	✓	✓	×
Remove selected samples (Ausgewählte Proben entfernen)	✓	✓	✓	×
Export, import, or remove external calibration (Externe Kalibrierung exportieren, importieren oder entfernen)	✓	✓	✓	×
Modify sample name (Probenname ändern)	✓	✓	✓	×
Modify sample type (Probentyp ändern)	✓	✓	✓	×
Modify sample ID (Proben-ID ändern)	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Modify actual concentration (Istkonzentration ändern)	✓	✓	✓	×
Modify dilution factor (Verdünnungsfaktor ändern)	✓	✓	✓	×
Modify comment fields (Kommentarfelder bearbeiten)	✓	✓	✓	×
Enable manual integration (Manuelle Integration aktivieren)	✓	✓	✓	×
Set peak to not found (Peak auf „nicht gefunden“ setzen)	✓	✓	✓	×
Include or exclude a peak from the results table (Einen Peak in die Ergebnistabelle aufnehmen oder ausschließen)	✓	✓	✓	×
Regression options (Regressionsoptionen)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Integrationsparameter für ein Einzelchromatogramm in der Ergebnistabelle ändern)	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Modify quantitation method for the results table component (Quantifizierungsmethode für Komponente der Ergebnistabelle modifizieren)	✓	✓	✓	×
Create metric plot new settings (Neue Einstellungen für metrische Darstellungen erstellen)	✓	✓	✓	✓
Add custom columns (Benutzerdefinierte Spalten hinzufügen)	✓	✓	✓	×
Set peak review title format (Titelformat für die Peak-Überprüfung festlegen)	✓	×	×	×
Remove custom column (Benutzerdefinierte Spalte entfernen)	✓	✓	×	×
Results table display settings (Einstellungen für die Anzeige der „Results Table“)	✓	✓	✓	✓
Lock results table (Ergebnistabelle sperren)	✓	✓	✓	✓
Unlock results table (Ergebnistabelle entsperren)	✓	×	×	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Mark results file as reviewed and save (Ergebnisdatei als „geprüft“ kennzeichnen und speichern)	✓	×	×	✓
Modify report template (Berichtsvorlage ändern)	✓	✓	×	×
Transfer results to LIMS (Ergebnisse in LIMS übertragen)	✓	✓	✓	×
Modify barcode column (Spalte „Barcode“ (Strichcode) ändern)	✓	✓	×	×
Change comparison sample assignment (Zuweisung der Vergleichsprobe ändern)	✓	✓	×	×
Add the MSMS spectra to library (MSMS-Spektren der Bibliothek hinzufügen)	✓	✓	×	×
Project default settings (Standardeinstellungen des Projekts)	✓	✓	×	×
Create report in all formats (Bericht in allen Formaten erstellen)	✓	✓	✓	✓
Edit flagging criteria parameters (Parameter für die Markierungskriterien bearbeiten)	✓	✓	✓	×

Tabelle 4-5: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Automatic outlier removal parameter change (Parameter für das automatische Entfernen von Ausreißern ändern)	✓	✓	×	×
Enable automatic outlier removal (Automatische Entfernung von Ausreißern aktivieren)	✓	✓	✓	×
Update processing method via FF/LS (Verarbeitungsmethode über FF/LS aktualisieren)	✓	✓	×	×
Update results via FF/LS (Ergebnisse über FF/LS aktualisieren)	✓	✓	×	×
Enable grouping by adducts functionality (Funktion der Gruppierung nach Addukten aktivieren)	✓	✓	×	×
Browse for files (Dateien suchen)	✓	✓	✓	✓
Enable standard addition (Standard-Addition aktivieren)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Prozentsatzregel für die manuelle Integration festlegen)	✓	×	×	×

Verwalten von Benutzern

Hinzufügen eines Benutzers oder einer Gruppe

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „Users“.
4. Klicken Sie auf **Add User** ( ).
   Das Dialogfeld „Select User or Group“ wird geöffnet.
5. Geben Sie den Namen des Benutzers oder der Gruppe ein und klicken Sie dann auf **OK**.

   Tipp! Für Informationen über das Dialogfeld „Select User or Group“ und seine Verwendung, klicken Sie auf **F1**.
6. Um den Benutzer zu aktivieren, stellen Sie sicher, dass das Kontrollkästchen **Active user or group** ausgewählt ist.
7. Wählen Sie im Bereich **Roles** eine oder mehrere Rollen aus und klicken Sie dann auf **Save**.

Deaktivieren von Benutzern oder Gruppen

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „Users“.
4. Wählen Sie aus der Liste **User name or group** den zu deaktivierenden Benutzer oder die zu deaktivierende Gruppe aus.
5. Deaktivieren Sie das Kontrollkästchen **Active user or group**.
   Die Software fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **Yes**.

Entfernen von Benutzern oder Gruppen

Gehen Sie nach diesem Verfahren vor, um einen Benutzer oder eine Gruppe aus der Software zu entfernen. Wenn ein Benutzer oder eine Gruppe aus Windows entfernt wird, muss der Benutzer auch aus SCIEX OS entfernt werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „Users“.
4. Wählen Sie aus der Liste **User name or group** den zu entfernenden Benutzer oder die zu entfernende Gruppe aus.
5. Klicken Sie auf **Delete**.
   Die Software fordert Sie zur Bestätigung auf.

6. Klicken Sie auf **OK**.

Verwalten von Rollen

Ändern der einem Benutzer oder einer Gruppe zugewiesenen Rolle

Mit diesem Verfahren können Sie einem Benutzer oder einer Gruppe neue Rollen zuweisen oder vorhandene Rollenzuweisungen entfernen.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „Users“.
4. Wählen Sie im Feld **User name or group** den zu ändernden Benutzer oder die zu ändernde Gruppe aus.
5. Wählen Sie die dem Benutzer oder der Gruppe zuzuweisenden Rollen aus und löschen Sie alle zu entfernenden Rollen.
6. Klicken Sie auf **Save**.

Erstellen einer benutzerdefinierten Rolle

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „Roles“.
4. Klicken Sie auf **Add Role** ( ).
   Das Dialogfeld „Duplicate a User Role“ wird geöffnet.
5. Wählen Sie im Feld **Existing user role** die Rolle aus, die als Vorlage für die neue Rolle verwendet werden soll.
6. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie dann auf **OK**.
7. Wählen Sie die Zugriffsberechtigungen für die Rolle aus.
8. Klicken Sie auf **Save All Roles**.
9. Klicken Sie auf **OK**.

Löschen einer benutzerdefinierten Rolle

Hinweis: Wenn ein Benutzer nur der zu löschenden Rolle zugewiesen ist, fordert das System zum Löschen des Benutzers sowie der Rolle auf.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „Roles“.

4. Klicken Sie auf **Delete a Role**.
   Das Dialogfeld „Delete a User Role“ wird geöffnet.
5. Wählen Sie die zu löschende Rolle aus und klicken Sie dann auf **OK**.

Einstellungen für die Benutzerverwaltung exportieren und importieren

Die SCIEX OS-Datenbank für die Benutzerverwaltung kann exportiert und importiert werden. Nachdem Sie die Datenbank für die Benutzerverwaltung beispielsweise auf einem SCIEX Computer konfiguriert haben, exportieren Sie sie und importieren Sie sie dann auf andere SCIEX Computer, um sicherzustellen, dass die Einstellungen für die Benutzerverwaltung übereinstimmen.

Es werden nur Domänenbenutzer exportiert. Lokale Benutzer werden nicht exportiert.

Vor dem Importieren von Einstellungen für die Benutzerverwaltung sichert die Software automatisch die aktuellen Einstellungen. Der Benutzer kann die letzte Datensicherung wiederherstellen.

Einstellungen für die Benutzerverwaltung exportieren

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Klicken Sie auf **Advanced** > **Export User Management settings**.
   Das Dialogfeld „Export User Management Settings“ wird geöffnet.
4. Klicken Sie auf **Browse**.
5. Navigieren Sie zu dem Ordner, in dem die Einstellungen gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie dann auf **Select Folder**.
6. Klicken Sie auf **Export**.
   Es wird eine Bestätigung mit dem Namen der Datei angezeigt, die die exportierten Einstellungen enthält.
7. Klicken Sie auf **OK**.

Einstellungen für die Benutzerverwaltung importieren

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Klicken Sie auf **Advanced** > **Import User Management settings**.
   Das Dialogfeld „Import User Management Settings“ wird geöffnet.
4. Klicken Sie auf **Browse**.
5. Navigieren Sie zu der Datei, die die zu importierenden Einstellungen enthält, wählen Sie sie aus, und klicken Sie dann auf **Open**.
   Die Software überprüft, ob die Datei gültig ist.

6. Klicken Sie auf **Import**.
   Die Software sichert die aktuellen Einstellungen für die Benutzerverwaltung und importiert die neuen Einstellungen. Eine Bestätigung wird angezeigt.
7. Klicken Sie auf **OK**.

Einstellungen für die Benutzerverwaltung wiederherstellen

Vor dem Importieren von Einstellungen für die Benutzerverwaltung sichert die Software die aktuellen Einstellungen. Verwenden Sie dieses Verfahren, um die letzte Sicherung der Einstellungen für die Benutzerverwaltung wiederherzustellen.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Öffnen Sie die Seite „User Management“.
3. Klicken Sie auf **Advanced** > **Restore previous settings**.
   Das Dialogfeld „Restore User Management Settings“ wird geöffnet.
4. Klicken Sie auf **Yes**.
5. Schließen Sie SCIEX OS und öffnen Sie es wieder.

Konfigurieren des Zugriffs auf Projekte und Projektdateien

Verwenden Sie die Windows-Sicherheitsfunktionen, um den Zugriff auf den Ordner „`SCIEX OS Data`“ zu steuern. Standardmäßig werden Projektdateien im Ordner „`SCIEX OS Data`“ gespeichert. Um auf ein Projekt zugreifen zu können, müssen die Benutzer Zugriff auf das Stammverzeichnis haben, in dem die Projektdaten gespeichert sind. Weitere Informationen finden Sie im Abschnitt: Windows-Sicherheitskonfiguration.

Projektordner

Jedes Projekt umfasst Ordner, in denen verschiedene Arten von Dateien gespeichert sind. Für Informationen über die Inhalte der verschiedenen Ordner siehe die Tabelle: Tabelle 4-6.

Tabelle 4-6: Projektordner

Ordner	Inhalt
`\Acquisition Methods`	Enthält die im Projekt erstellten Massenspektrometer (MS)- und LC-Methoden. MS-Methoden haben die Erweiterung .msm und LC-Methoden die Erweiterung .lcm.
`\Audit Data`	Enthält die Projekt-Audit-Map und alle Audit-Aufzeichnungen.
`\Batch`	Enthält alle Erfassungschargendateien, die gespeichert wurden. Erfassungschargen haben die Erweiterung .bch.

Tabelle 4-6: Projektordner (Fortsetzung)

Ordner	Inhalt
\Data	Enthält die Dateien mit den Erfassungsdaten. Erfassungsdatendateien haben die Erweiterungen .wiff und .wiff2.
\Project Information	Enthält die Dateien für die Projektstandardeinstellungen.
\Quantitation Methods	Enthält alle Dateien mit den Verarbeitungsmethoden. Verarbeitungsmethoden haben die Erweiterung .qmethod.
\Quantitation Results	Enthält alle Dateien der Quantifizierungs-„Results Table“. „Results Table“-Dateien haben die Erweiterung .qsession.

Software-Dateitypen

Für gängige SCIEX OS-Dateitypen siehe die Tabelle: Tabelle 4-7.

Tabelle 4-7: SCIEX OS-Dateien

Erweiterung	Dateityp	Ordner
atds	• Daten und Archive des Workstation-Audit-Trails • Einstellungen des Workstation-Audit-Trails • Daten und Archive des Projekt-Audit-Trails • Einstellungen des Projekt-Audit-Trails	• Für Projekte: „*<project name>*\Audit Data“ • Für die Workstation: C:\ProgramData\SCIEX\Audit Data
atms	Audit-Maps	• Für Projekte: „*<project name>*\Audit Data“ • Für die Workstation: C:\ProgramData\SCIEX\Audit Data
bch	Charge	Batch
cset	Einstellungen der „Results Table“	Project Information
dad	Datei mit Massenspektrometriedaten	• Optimization • Data
exml	Standardeinstellungen des Projekts	Project Information

Tabelle 4-7: SCIEX OS-Dateien (Fortsetzung)

Erweiterung	Dateityp	Ordner
journal	Temporäre Dateien, die von SCIEX OS erstellt werden	Verschiedene Ordner
lcm	LC-Methode	`Acquisition Methods`
msm	MS-Methode	`Acquisition Methods`
pdf	Daten im PDF-Format	—
qlayout	Arbeitsbereich-Layout	— **Hinweis:** Das übliche Arbeitsbereich-Layout für ein Projekt ist im Verzeichnis „`Project Information`“ gespeichert.
qmethod	Verarbeitungsmethode	`Quantitation Methods`
qsession	„Results Table“ **Hinweis:** SCIEX OS kann nur qsession-Dateien öffnen, die mit SCIEX OS erstellt wurden.	`Quantitation Results`
wiff	Datei mit Massenspektrometriedaten, die mit der SCIEX OS-Software kompatibel ist. **Hinweis:** SCIEX OS erzeugt wiff- und wiff2-Dateien.	`Data`
wiff.scan	Datei mit Massenspektrometriedaten	• `Optimization` • `Data`
wiff2	Datei mit Massenspektrometriedaten, die von SCIEX OS erzeugt wurden	• `Optimization` • `Data`
xls oder xlsx	Excel-Tabelle	`Batch`
xps	Neukalibrierung	`Data\Cal`

Central Administrator Console 5

Die Central Administrator Console (CAC) Software ist eine optionale Alternative zur lokalen Verwaltung mit der SCIEX OS Software. Die CAC Software beinhaltet eine zentrale Verwaltung und Anpassung von Rollen, Benutzern, Workstations und Arbeitsgruppen in einer Anwendung.

Dieser Abschnitt beschreibt die CAC Software und erklärt, wie man diese zur zentralen Verwaltung von Personen, Projekten und Workstations konfiguriert und verwendet.

Hinweis: Um die CAC Software zu verwenden und Workstations am Server zu registrieren, muss sichergestellt werden, dass die SCIEX OS Software auf jeder Workstation installiert ist.

Die CAC Software wird per Lizenz aktiviert und kann auf jeder Workstation installiert werden, die SCIEX OS Version 3.0 und Windows Server 2019 unterstützt.

Die CAC Software ist im SCIEX OS Installationspaket enthalten. Die CAC Software und SCIEX OS können jedoch nicht auf derselben Workstation installiert werden.

Benutzer

Verwenden Sie die Seite „User Management“, um Windows Benutzer und Gruppen zur Datenbank für die Benutzerverwaltung für SCIEX OS hinzuzufügen. Zudem kann der Administrator Benutzerrollen im Abschnitt „User Roles and Permissions“ hinzufügen, ändern und löschen. Für den Zugriff auf die Software müssen Benutzer in der Datenbank für die Benutzerverwaltung definiert sein oder müssen ein Mitglied einer in der Datenbank definierten Gruppen sein.

Benutzer-Pool

Ausschließlich autorisierte Benutzer können sich bei der Workstation anmelden und auf SCIEX OS zugreifen, wenn SCIEX OS mit der Central Administrator Console (CAC) Software verwaltet wird. Bevor Benutzer zu Arbeitsgruppen hinzugefügt werden können, müssen diese zum Benutzer-Pool hinzugefügt werden.

Benutzer oder Gruppe zum „User Pool“ hinzufügen

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „User Pool“.
4. Klicken Sie auf **Add users to the User Pool** ( ).
   Das Dialogfeld „Select Users or Groups“ wird geöffnet.
5. Geben Sie den Namen des Benutzers oder der Gruppe ein und klicken Sie dann auf **OK**.

Tipp! Halten Sie die **Ctrl**-Taste gedrückt und klicken Sie dann auf **OK**, um mehrere Benutzer oder Gruppen auszuwählen.

Benutzer oder Gruppen löschen

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „User Pool“.
4. Wählen Sie im rechten Fensterbereich den zu löschenden Benutzer oder die zu löschende Gruppe aus und klicken Sie dann auf **Delete**.
   Die Software fordert Sie zur Bestätigung auf.
5. Klicken Sie auf **OK**.

Benutzerrollen und Berechtigungen

In diesem Abschnitt wird die Seite „User Roles and Permissions“ beschrieben.

Benutzer können einer oder mehreren vordefinierten Rollen, die in der folgenden Tabelle beschrieben werden, oder auch benutzerdefinierten Rollen zugewiesen werden, falls dies erforderlich ist. Die Funktionen, auf die der Benutzer zugreifen kann, werden durch Rollen festgelegt. Die vordefinierten Rollen können nicht gelöscht und ihre Berechtigungen nicht geändert werden.

Tabelle 5-1: Vordefinierte Rollen

Rolle	Typische Aufgaben
Administrator (Administrator)	• Verwaltet das System. • Konfiguriert die Sicherheit.
Method Developer (Methodenentwickler)	• Erstellt Methoden. • Führt Chargen aus. • Analysiert Daten zur Verwendung durch den Endbenutzer.
Analyst (Analyst)	• Führt Chargen aus. • Analysiert Daten zur Verwendung durch den Endbenutzer.
Reviewer (Prüfer)	• Prüft Daten. • Prüft Audit-Trails. • Bewertet Quantifizierungsergebnisse.

Tabelle 5-2: Voreingestellte Berechtigungen

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Batch (Charge)				
Submit unlocked methods (Entsperrte Methoden übergeben)	✓	✓	✓	×
Open (Öffnen)	✓	✓	✓	✓
Save as (Speichern unter)	✓	✓	✓	×
Submit (Übergeben)	✓	✓	✓	×
Save (Speichern)	✓	✓	✓	×
Save ion reference table (Ionenreferenztabelle speichern)	✓	✓	✓	×
Add data sub-folders (Daten-Unterordner hinzufügen)	✓	✓	✓	×
Configure Decision Rules (Entscheidungsregeln konfigurieren)	✓	✓	✓	×
Configuration (Konfiguration)				
General tab (Registerkarte „Allgemein“)	✓	✓	×	×
General: change regional setting (Allgemein: Regionseinstellungen ändern)	✓	✓	×	×
General: full screen mode (Allgemein: Vollbildmodus)	✓	✓	×	×
LIMS communication tab (Registerkarte „LIMS-Kommunikation“)	✓	✓	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
General:Stop Windows services(Allgemein: Windows Services stoppen)	✓	×	×	×
Audit maps tab (Registerkarte „Audit-Maps“)	✓	×	×	×
Queue tab (Registerkarte „Warteschlange“)	✓	✓	✓	✓
Queue: instrument idle time (Warteschlange: Geräteleerlaufzeit)	✓	✓	×	×
Queue: max number of acquired samples (Warteschlange: Maximale Anzahl erfasster Proben)	✓	✓	×	×
Queue: other queue settings (Warteschlange: Andere Warteschlangeneinstellungen)	✓	✓	×	×
Projects tab (Registerkarte „Projekte“)	✓	✓	✓	✓
Projects: create project (Projekte: Projekt erstellen)	✓	✓	✓	×
Projects: apply an audit map template to an existing project (Projekte: Eine Audit-Map-Vorlage auf ein bestehendes Projekt anwenden)	✓	×	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Projects: create root directory (Projekte: Stammverzeichnis erstellen)	✓	×	×	×
Projects: set current root directory (Projekte: Aktuelles Stammverzeichnis festlegen)	✓	×	×	×
Projects: specify network credentials (Projekte: Netzwerkanmeldedaten festlegen)	✓	×	×	×
Projects: Enable checksum writing for wiff1 data creation (Projekte: Das Schreiben der Prüfsumme für die wiff1-Datenerstellung aktivieren)	✓	×	×	×
Projects: clear root directory (Projekte: Stammverzeichnis löschen	✓	×	×	×
Devices tab (Registerkarte „Geräte“)	✓	✓	✓	×
User management tab (Registerkarte „Benutzerverwaltung“)	✓	×	×	×
Force user logoff (Abmeldung des Benutzers erzwingen)	✓	×	×	×
Event Log (Ereignisprotokoll)				
Access event log workspace (Auf Arbeitsbereich „Ereignisprotokoll“ zugreifen)	✓	✓	✓	✓

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Archive log (Ereignisprotokoll archivieren)	✓	✓	✓	✓
Audit Trail (Audit-Trail)				
Access audit trail workspace (Auf Arbeitsbereich „Audit-Trail“ zugreifen)	✓	✓	✓	✓
View active audit map (Aktive Audit-Map anzeigen)	✓	✓	✓	✓
Print/Export audit trail (Audit-Trail drucken/ exportieren)	✓	✓	✓	✓
Data Acquisition Panel (Teilfenster „Datenerfassung“)				
Start (Start)	✓	✓	✓	×
Stop (Stopp)	✓	✓	✓	×
Save (Speichern)	✓	✓	✓	×
MS & LC Method (MS & LC Methode)				
Access method workspace (Auf Arbeitsbereich „Methode“ zugreifen)	✓	✓	✓	✓
New (Neu)	✓	✓	×	×
Open (Öffnen)	✓	✓	✓	✓
Save (Speichern)	✓	✓	×	×
Save as (Speichern unter)	✓	✓	×	×
Lock/Unlock method (Methode sperren/ entsperren)	✓	✓	×	×
Queue (Warteschlange)				
Manage (Verwalten)	✓	✓	✓	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Start/Stop (Start/ Stopp)	✓	✓	✓	×
Print (Drucken)	✓	✓	✓	✓
Library (Bibliothek)				
Access library workspace (Auf Arbeitsbereich „Bibliothek“ zugreifen)	✓	✓	✓	✓
CAC settings (CAC Client)				
Enable Central Administration (Zentraladministration aktivieren)	✓	×	×	×
MS Tune (MS Tune)				
Access MS Tune workspace (Auf Arbeitsbereich „MS-Tune“ zugreifen)	✓	✓	✓	×
Advanced MS Tuning (Erweitertes MS-Tuning)	✓	✓	×	×
Advanced troubleshooting (Erweiterte Fehlerbehebung)	✓	✓	×	×
Quick status check (Schnelle Statusüberprüfung)	✓	✓	✓	×
Restore instrument data (Gerätedaten wiederherstellen)	✓	✓	×	×
Analytics (Analyse)				
New results (Neue Ergebnisse)	✓	✓	✓	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Create processing method (Verarbeitungsmethode erstellen)	✓	✓	✓	×
Modify processing method (Verarbeitungsmethode ändern)	✓	✓	×	×
Allow Export and Create Report of unlocked Results Table (Export nicht gesperrter „Results Table“ und Erstellen eines Berichts aus dieser erlauben)	✓	×	×	×
Save results for Automation Batch (Ergebnisse speichern für Automatisierungs-Charge)	✓	✓	✓	×
Change default quantitation method integration algorithm (Integrationsalgorithmus der standardmäßigen Quantifizierungsmethode ändern)	✓	✓	×	×
Change default quantitation method integration parameters (Integrationsparameter der standardmäßigen Quantifizierungsmethode ändern)	✓	✓	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Enable project modified peak warning (Warnung bei veränderten Peaks eines Projekts aktivieren)	✓	×	×	×
Add samples (Proben hinzufügen)	✓	✓	✓	×
Remove selected samples (Ausgewählte Proben entfernen)	✓	✓	✓	×
Export, import, or remove external calibration (Externe Kalibrierung exportieren, importieren oder entfernen)	✓	✓	✓	×
Modify sample name (Probenname ändern)	✓	✓	✓	×
Modify sample type (Probentyp ändern)	✓	✓	✓	×
Modify sample ID (Proben-ID ändern)	✓	✓	✓	×
Modify actual concentration (Istkonzentration ändern)	✓	✓	✓	×
Modify dilution factor (Verdünnungsfaktor ändern)	✓	✓	✓	×
Modify comment fields (Kommentarfelder bearbeiten)	✓	✓	✓	×
Enable manual integration (Manuelle Integration aktivieren)	✓	✓	✓	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Set peak to not found (Peak auf „nicht gefunden“ setzen)	✓	✓	✓	×
Include or exclude a peak from the results table (Einen Peak in die Ergebnistabelle aufnehmen oder ausschließen)	✓	✓	✓	×
Regression options (Regressionsoptionen)	✓	✓	✓	×
Modify results table integration parameters for a single chromatogram (Integrationsparameter für ein Einzelchromatogramm in der Ergebnistabelle ändern)	✓	✓	✓	×
Modify quantitation method for the results table component (Quantifizierungsmethode für Komponente der Ergebnistabelle modifizieren)	✓	✓	✓	×
Create metric plot new settings (Neue Einstellungen für metrische Darstellungen erstellen)	✓	✓	✓	✓
Add custom columns (Benutzerdefinierte Spalten hinzufügen)	✓	✓	✓	×
Set peak review title format (Titelformat für die Peak-Überprüfung festlegen)	✓	×	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Remove custom column (Benutzerdefinierte Spalte entfernen)	✓	✓	×	×
Results table display settings (Einstellungen für die Anzeige der „Results Table“)	✓	✓	✓	✓
Lock results table (Ergebnistabelle sperren)	✓	✓	✓	✓
Unlock results table (Ergebnistabelle entsperren)	✓	×	×	×
Mark results file as reviewed and save (Ergebnisdatei als „geprüft“ kennzeichnen und speichern)	✓	×	×	✓
Modify report template (Berichtsvorlage ändern)	✓	✓	×	×
Transfer results to LIMS (Ergebnisse in LIMS übertragen)	✓	✓	✓	×
Modify barcode column (Spalte „Barcode“ (Strichcode) ändern)	✓	✓	×	×
Change comparison sample assignment (Zuweisung der Vergleichsprobe ändern)	✓	✓	×	×
Add the MSMS spectra to library (MSMS-Spektren der Bibliothek hinzufügen)	✓	✓	×	×

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Project default settings (Standardeinstellungen des Projekts)	✓	✓	×	×
Create report in all formats (Bericht in allen Formaten erstellen)	✓	✓	✓	✓
Edit flagging criteria parameters (Parameter für die Markierungskriterien bearbeiten)	✓	✓	✓	×
Automatic outlier removal parameter change (Parameter für das automatische Entfernen von Ausreißern ändern)	✓	✓	×	×
Enable automatic outlier removal (Automatische Entfernung von Ausreißern aktivieren)	✓	✓	✓	×
Update processing method via FF/LS (Verarbeitungsmethode über FF/LS aktualisieren)	✓	✓	×	×
Update results via FF/LS (Ergebnisse über FF/LS aktualisieren)	✓	✓	×	×
Enable grouping by adducts functionality (Funktion der Gruppierung nach Addukten aktivieren)	✓	✓	×	×
Browse for files (Dateien suchen)	✓	✓	✓	✓

Tabelle 5-2: Voreingestellte Berechtigungen (Fortsetzung)

Berechtigung	Administrator	Method Developer	Analyst	Reviewer
Enable standard addition (Standard-Addition aktivieren)	✓	✓	✓	×
Set Manual Integration Percentage Rule (Prozentsatzregel für die manuelle Integration festlegen)	✓	×	×	×
Explorer (Explorer)				
Access explorer workspace (Auf Arbeitsbereich „Explorer“ zugreifen)	✓	✓	✓	✓
Export (Exportieren)	✓	✓	✓	×
Print (Drucken)	✓	✓	✓	×
Options (Optionen)	✓	✓	✓	×
Recalibrate (Rekalibrieren)	✓	✓	×	×

Hinzufügen einer benutzerdefinierten Rolle

Die Central Administrator Console (CAC) Software verfügt über vier vordefinierte Rollen. Wenn weitere benötigt werden, dann kopieren Sie eine vorhandene Rolle und weisen Sie dieser Zugriffsrechte zu.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „User Roles and Permissions“.
4. Klicken Sie auf **Add Role** ( ).
   Das Dialogfeld „Duplicate a User Role“ wird geöffnet.
5. Wählen Sie im Feld **Existing user role** die Rolle aus, die als Vorlage für die neue Rolle verwendet werden soll.
6. Geben Sie einen Namen und eine Beschreibung für die Rolle ein und klicken Sie dann auf **OK**.
   Die neue Rolle wird im Fenster „User Roles and Permission Categories“ angezeigt.

7. Wählen Sie die Zugriffsberechtigungen für die Rolle aus, indem Sie die entsprechenden Kontrollkästchen aktivieren.
8. Klicken Sie auf **Save All Roles**.

Löschen einer benutzerdefinierten Rolle

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „User Management“.
3. Öffnen Sie die Registerkarte „User Roles and Permissions“.
4. Klicken Sie auf **Delete a Role**.
   Das Dialogfeld „Delete a User Role“ wird geöffnet.
5. Wählen Sie die zu löschende Rolle aus und klicken Sie dann auf **OK**.

Arbeitsgruppen

Verwenden Sie die Seite „Workgroup Management“ zum Verwalten von Arbeitsgruppen. Arbeitsgruppen umfassen Benutzer, Workstations und Projekte.

Erstellen Sie eine Arbeitsgruppe, indem Sie Ressourcen von ihren jeweiligen Pools hinzufügen. Bevor Sie Arbeitsgruppen erstellen, stellen Sie sicher, dass Sie alle potenziellen Nutzer zum „User Pool“, Workstations zum „Workstation Pool“ und Projektstammverzeichnisse zum „Project Pool“ hinzufügen.

Fügen Sie ggf. zusätzliche Rollen hinzu. Wählen Sie optional den Sicherheitsmodus für jede Arbeitsgruppe aus.

Die „Security Mode“-Einstellung für die Arbeitsgruppe hat Vorrang vor der „Security Mode“-Einstellung für die Workstation, wenn die Workstation bei der Central Administrator Console (CAC) Software registriert und Mitglied der Arbeitsgruppe ist.

Fügen Sie keine lokalen Benutzer zu Arbeitsgruppen hinzu. Die CAC Software ist eine Netzwerkanwendung und nur Netzwerkbenutzer sollten zu einer Arbeitsgruppe hinzugefügt werden.

Hinweis: In jeder Arbeitsgruppe sollte mindestens einem Benutzer Folgendes zugewiesen werden: Administrator-Rolle. Nur ein Administrator oder Supervisor kann den CAC Software-Bildschirm entsperren, wenn der aktuell angemeldete Benutzer nicht verfügbar ist.

Wenn Server-basierte Sicherheit für eine bestimmte Workstation nicht mehr erforderlich ist, dann verwalten Sie die Sicherheit für diese Workstation lokal über SCIEX OS.

Erstellen einer Arbeitsgruppe

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Klicken Sie auf **Add Workgroup** ().

Das Dialogfeld „Add a Workgroup“ wird geöffnet.

4. Geben Sie im Feld **Workgroup Name** einen Namen ein.
5. Geben Sie eine Beschreibung in das Feld **Description** ein und klicken dann auf **Add**.
   Die Arbeitsgruppe wird erstellt und dem Teilfenster „Manage Workgroups and Assignments“ hinzugefügt. Die Central Administrator Console (CAC) Software erstellt die entsprechende Arbeitsgruppe auf dem Server.

Hinweis: „Integrated Mode“ ist die standardmäßige Sicherheitseinstellung.

Eine Arbeitsgruppe löschen

Wenn eine Arbeitsgruppe nicht länger benötigt wird, dann löschen Sie diese aus der Liste „Workgroup“. Das Löschen einer Arbeitsgruppe entfernt die Arbeitsgruppe nur aus der Central Administrator Console (CAC) Software. Auf der Workstation gehen keine Daten verloren.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Erweitern Sie die Liste **Workgroups** und suchen Sie die zu löschende Arbeitsgruppe. Klicken Sie auf **Delete**.
   Das Dialogfeld „Delete Workgroup“ wird geöffnet.
4. Klicken Sie auf **Yes**.

Benutzer oder Gruppen einer Arbeitsgruppe hinzufügen

Hinweis: Den zur Arbeitsgruppe hinzugefügten Benutzern wird nicht automatisch eine Rolle zugewiesen. Um Benutzern Rollen zuzuweisen, siehe Abschnitt: Hinzufügen oder Entfernen einer Rolle.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Erweitern Sie im Teilfenster „Manage Workgroups and Assignments“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Users**.
4. Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie dann auf **Add** ().

   Tipp! Sie können mehrere Benutzer durch Drücken von **Shift** hinzufügen oder auswählen und dann die gewünschten Benutzer auswählen.

   Der Benutzer bzw. die Gruppe wird zur aktuellen Arbeitsgruppe hinzugefügt.
5. Weisen Sie dem hinzugefügten Benutzer bzw. der Gruppe eine oder mehrere Rollen zu. Siehe Abschnitt: Hinzufügen oder Entfernen einer Rolle.
6. Klicken Sie auf **Save**.

Hinzufügen oder Entfernen einer Rolle

Voraussetzungen
• Benutzer oder Gruppen einer Arbeitsgruppe hinzufügen.

Informationen über das Erstellen von Rollen in der Central Administrator Console (CAC) Software finden Sie im Abschnitt: Hinzufügen einer benutzerdefinierten Rolle. Benutzer oder Gruppen mit einer zugewiesenen Rolle besitzen alle der Rolle zugeordneten Berechtigungen. Benutzer oder Gruppen können über mehr als eine Rolle gleichzeitig verfügen.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Erweitern Sie im Teilfenster „Manage Workgroups and Assignments“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Users**.
4. Im Abschnitt „Current Workgroup Membership“ können Sie Rollen in der Spalte **Assign Roles** zuweisen oder entfernen.
5. Klicken Sie auf **Save**.

Workstations einer Arbeitsgruppe hinzufügen

Hinweis: Eine Workstation wird im Workstation Pool nur dann angezeigt, wenn sie bei der Central Administrator Console (CAC) Software registriert ist. Siehe Abschnitt: Hinzufügen einer Workstation

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Erweitern Sie im Teilfenster „Manage Workgroups and Assignments“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Workstations**.
4. Wählen Sie eine Workstation aus und klicken Sie dann auf **Add** ().
   Die Workstation wird zur aktuellen Arbeitsgruppe hinzugefügt.
5. Klicken Sie auf **Save**.

Arbeitsgruppen-Sicherheitseinstellungen zuweisen

Voraussetzungen
• Hinzufügen einer Workstation • Workstations einer Arbeitsgruppe hinzufügen

Informationen über Sicherheitsmodi finden Sie im Abschnitt: Konfigurieren des Sicherheitsmodus.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Erweitern Sie im Teilfenster „Manage Workgroups and Assignments“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Workstations**.
4. (Optional) Um die aktuelle Arbeitsgruppe als Standard-Arbeitsgruppe für diese Workstation festzulegen, aktivieren Sie das Kontrollkästchen **Set Default** im Abschnitt „Current Workgroup Membership“.
5. Wählen Sie im Abschnitt „Assign Security Settings“ den **Security mode** für die Arbeitsgruppe aus und geben Sie dann die entsprechenden **Screen lock**- und **Auto logoff**-Zeiten ein.
6. Klicken Sie auf **Save**.

Projekte einer Arbeitsgruppe hinzufügen

Hinweis: Dieses Verfahren ist nur erforderlich, wenn der Projektzugriff zentral verwaltet wird.

Hinweis: Wenn ein Projekt zu mehr als einer Arbeitsgruppe hinzugefügt wird, dann werden die Benutzerberechtigungen zum Projekt angehängt aber nicht überschrieben. Zum Beispiel enthält Workgroup 1 den User A, User B und das Project_01. Workgroup 2 enthält den User B und User C. Wenn Project_01 zur Workgroup 2 hinzugefügt wird, dann erhalten User A, User B und User C Zugriff auf das Project_01.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workgroup Management“.
3. Erweitern Sie im Teilfenster „Manage Workgroups and Assignments“ die Arbeitsgruppe, die geändert werden soll, und erweitern Sie dann die Liste **Projects**.
4. Aktivieren Sie das Kontrollkästchen **Use central settings for projects**.
   Der Abschnitt zur Projektauswahl wird angezeigt.
5. Wählen Sie ein **Project root directory** aus, um eine ganze Projektgruppe hinzuzufügen oder erweitern Sie den Projektstamm und wählen Sie ein bestimmtes Projekt zum Hinzufügen zur Arbeitsgruppe aus.
6. Klicken Sie auf **Add** (), um die Projekte zur Arbeitsgruppe hinzuzufügen.
   Der Projektstamm wird zur Tabelle „Current Workgroup Membership“ hinzugefügt. Erweitern Sie den Projektstamm, um die aktuellen Projekte in der Arbeitsgruppe anzuzeigen.
7. Klicken Sie auf **Save**.

Projekte verwalten

Verwenden Sie die Seite „Project Management“ zum Erstellen, Ändern und Löschen von Projekten.

Um auf ein Projekt zugreifen zu können, müssen die Benutzer Zugriff auf das Stammverzeichnis haben, in dem die Projektdaten gespeichert sind. Weitere Informationen finden Sie im Abschnitt: Über Projekte und Stammverzeichnisse.

Über Projekte und Stammverzeichnisse

Ein Stammverzeichnis ist ein Ordner, der ein oder mehrere Projekte enthält. Dies ist der Ordner, in dem die Software nach Projektdaten sucht. Das vordefinierte Stammverzeichnis ist `D:\SCIEX OS Data`.

Um sicherzustellen, dass Projektinformationen sicher gespeichert werden, erstellen Sie Projekte mithilfe der Central Administrator Console (CAC) Software. Fügen Sie Projekte zum „Project Root Pool“ hinzu, bevor Sie sie zu einer Arbeitsgruppe hinzufügen. Siehe Abschnitt: Hinzufügen eines Projekts.

Projektdaten können in Unterordnern organisiert werden. Erstellen Sie die Unterordner mit der CAC Software. Siehe Abschnitt: Hinzufügen eines Unterordners.

Hinweis: Wenn ein Projekt außerhalb der CAC Software erstellt wird, dann sollte der Projektstamm nach dem Erstellen des Projekts aktualisiert werden. Wenn der Stamm aktualisiert wird, dann werden die Inhalte des „Project Root Pool“ mit dem Inhalt der Projekt-Stammverzeichnisse im Netzwerk synchronisiert.

Hinzufügen eines Stammverzeichnisses

Ein Stammverzeichnis ist der Ordner, in dem ein oder mehrere Projekte gespeichert werden.

Hinweis: Die Software speichert bis zu zehn Stammverzeichnisse.

Tipp! Lokale Laufwerke sind nicht über das Netzwerk zugänglich. Ein Stammverzeichnis kann nur auf einem freigegebenen Laufwerk erstellt werden.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Project Management“.
3. Klicken Sie auf **Add new or existing project root to project pool** ( ).
   Das Dialogfeld „Add Root Directory“ wird geöffnet.
4. Geben Sie den vollständigen Pfad zum Stammverzeichnis ein und klicken Sie dann auf **OK**.
   Der Ordner wird erstellt.

   Tipp! Statt den Pfad einzugeben, klicken Sie auf **Browse** und wählen Sie den Ordner aus, in dem das Stammverzeichnis erstellt werden soll.

   Tipp! Erstellen Sie alternativ einen Ordner im Datei-Explorer, suchen Sie diesen Ordner und wählen Sie ihn aus.

Hinweis: Bei SCIEX OS-Installationen mit einer Verarbeitungslizenz kann das Stammverzeichnis ein Ordner der Analyst Software (`Analyst Data\Projects`) sein.

5. Klicken Sie auf **OK**.
   Das neue Stammverzeichnis wird zum Stammverzeichnis für das aktuelle Projekt.

Löschen eines Projekt-Stammverzeichnisses

Die Software führt eine Liste der letzten zehn verwendeten Stammverzeichnisse. Der Benutzer kann Stammverzeichnisse aus dieser Liste löschen.

Hinweis: Durch das Löschen eines Projekt-Stammverzeichnisses werden ebenfalls alle zugehörigen Projekte aus dem Projektstammpool gelöscht.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Project Management“.
3. Suchen Sie das zu löschende Projekt-Hauptverzeichnis und klicken Sie dann auf **Delete Project Root** im Abschnitt „Actions“.
   Die Software fordert Sie zur Bestätigung auf.
4. Klicken Sie auf **OK**.

Hinzufügen eines Projekts

Voraussetzungen
• Hinzufügen eines Stammverzeichnisses

Im Projekt werden Erfassungsmethoden, Daten, Chargen, Verarbeitungsmethoden, Verarbeitungsergebnisse usw. gespeichert. Wir empfehlen, einen separaten Projektordner für jedes Projekt zu verwenden.

Außerhalb der Central Administrator Console (CAC) Software sollten Sie keine Projekte erstellen oder Dateien kopieren oder einfügen.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Project Management“.
3. Klicken Sie auf **Add project** im Abschnitt „Actions“ des Stammordners.
   Das Dialogfeld „New Project“ öffnet sich.
4. Geben Sie den Projektnamen ein.
5. Klicken Sie auf **OK**.
   Das neue Projekt wird unter dem Projektstamm angezeigt.

Hinzufügen eines Unterordners

Daten in Projekten können in Unterordnern weitergehend organisiert werden.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Project Management“.
3. Klicken Sie auf **Add data sub-folders** im Abschnitt „Actions“ des Stammordners.
   Das Dialogfeld „Add Data Sub-Folders“ wird geöffnet.
4. Wählen Sie ein Projekt aus, zu dem der Unterordner gehören soll.
5. Klicken Sie auf **Add a new data sub-folder** ( ).
   Das Dialogfeld „Data Sub-Folder Name“ wird geöffnet.
6. Geben Sie den Namen des Unterordners ein.
7. Klicken Sie auf **Save**.

   Tipp! Unterordner können innerhalb anderer Unterordner geschachtelt werden. Um einen geschachtelten Unterordner zu erstellen, wählen Sie einen vorhandenen Unterordner im Abschnitt „Project Data Sub-Folders“ aus und klicken Sie dann auf **Add a new data sub-folder** ( ).
8. Schließen Sie das Dialogfeld „Add Data Sub-Folders“.

Workstations

Verwenden Sie die Seite „Workstation Management“ zum Verwalten sämtlicher mit dem CAC Server verbundenen Workstations. Auf Workstations, die über die CAC Software gesteuert werden, werden automatisch benutzerdefinierte Einstellungen angewendet.

Hinzufügen einer Workstation

Auf der Seite „Workstation Management“ können Administratoren Workstations zur Steuerung durch die Central Administrator Console (CAC) Software hinzufügen oder entfernen.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workstation Management“.
3. Klicken Sie auf **Add Workstation to the Workstations Pool** ( ).
   Das Dialogfeld „Select Computers“ wird geöffnet.
4. Geben Sie die Namen der Workstations ein, die hinzugefügt werden sollen, und klicken Sie dann auf **OK**.

Löschen einer Workstation

Wird eine Workstation nicht mehr gebraucht oder ist in einer Arbeitsgruppe nicht mehr erforderlich, dann löschen Sie diese aus dem Workstation Pool. Das Löschen einer

Workstation entfernt diese aus allen Arbeitsgruppen, denen sie zugewiesen wurde. Auf der Workstation gehen keine Daten verloren, wenn sie entfernt wird.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Öffnen Sie die Seite „Workstation Management“.
3. Klicken Sie auf **Workstation Management**.
4. Suchen Sie im Teilfenster „Workstation Pool“ die zu löschende Workstation und klicken Sie dann auf **Delete**.
   Das Dialogfeld „Delete Workstation“ wird geöffnet.
5. Klicken Sie auf **OK**.

Berichte und Sicherheitsfunktionen

Arbeitsgruppen-Datenberichte erstellen

Benutzer können Datenberichte erstellen, die Details wie beispielsweise konfigurierte Benutzer, Rollen, Workstations, Projekte und Arbeitsgruppen enthalten.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Klicken Sie auf **Print**.
   Das Dialogfeld „Print“ wird geöffnet.
3. Stellen Sie die Druckoptionen ein und klicken Sie dann auf **Print**.
4. (Nur als PDF drucken) Navigieren Sie zu dem Speicherort, an dem der Bericht gespeichert werden soll und klicken Sie dann auf **Save**.

Einstellungen für die CAC Software exportieren

Der Benutzer kann Sicherheitseinstellungen exportieren, die auf einen anderen Central Administrator Console (CAC) Server angewendet werden können. Diese Einstellungen werden als eine ecac-Datei exportiert.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Klicken Sie auf **Advanced** > **Export CAC settings**.
   Das Dialogfeld „Export CAC Settings“ wird geöffnet.
3. Klicken Sie auf **Browse**.
4. Navigieren Sie zu dem Ordner, in dem die Einstellungen gespeichert werden sollen, wählen Sie ihn aus, und klicken Sie dann auf **Select Folder**.
5. Klicken Sie auf **Export**.
   Es wird eine Bestätigung mit dem Namen der Datei angezeigt, die die exportierten Einstellungen enthält.
6. Klicken Sie auf **OK**.

Einstellungen der CAC Software importieren

Voraussetzungen
• Einstellungen für die CAC Software exportieren

Der Benutzer kann Sicherheitseinstellungen von SCIEX OS oder anderen Central Administrator Console (CAC) Servern importieren. Diese Einstellungen werden aus einer ecac-Datei importiert.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Klicken Sie auf **Advanced** > **Import CAC settings**.
   Das Dialogfeld „Import CAC Settings“ wird geöffnet.
3. Klicken Sie auf **Browse**.
4. Navigieren Sie zu der Datei, die die zu importierenden Einstellungen enthält, wählen Sie sie aus, und klicken Sie dann auf **Open**.
   Die Software stellt sicher, dass die Datei gültig ist.
5. Klicken Sie auf **Import**.
   Die Software sichert die aktuellen Einstellungen und importiert die neuen Einstellungen. Eine Bestätigung wird angezeigt.

   Hinweis: Die importierten Einstellungen werden nach dem Neustart der CAC Software übernommen.
6. Klicken Sie auf **OK**.

CAC-Software-Einstellungen wiederherstellen

Der Benutzer kann die zuletzt exportierten ecac-Einstellungen automatisch importieren.

1. Öffnen Sie den Arbeitsbereich „Central Administration“.
2. Klicken Sie auf **Advanced** > **Restore CAC settings**.
   Das Dialogfeld „Restore CAC Settings“ wird geöffnet.

   Hinweis: Die wiederhergestellten Einstellungen werden nach dem Neustart der Central Administrator Console (CAC) Software übernommen.
3. Klicken Sie auf **Yes**.

Netzwerkerfassung 6

In diesem Abschnitt werden die Funktionsweise der Netzwerkerfassung in SCIEX OS und die Vorteile und Grenzen netzwerkbasierter Projekte beschrieben. Darüber hinaus werden auch Verfahren für die Konfiguration der Netzwerkerfassung beschrieben.

Über die Netzwerkerfassung

Die Netzwerkerfassung kann verwendet werden, um Daten aus einem oder mehreren Gerät(en) in netzwerkbasierten Projektordnern zu erfassen, die auf Remote-Arbeitsplätzen verarbeitet werden können. Dieser Prozess ist Netzwerkfehlern gegenüber tolerant und stellt sicher, dass keine Daten verloren gehen, wenn die Netzwerkverbindung während der Erfassung ausfällt.

Bei der Verwendung von Netzwerkprojekten kann die Systemleistung langsamer sein als bei der Verwendung lokaler Projekte. Da sich in den Netzwerkordnern auch einige Audit-Trails befinden, ist jede Aktion, die eine Projekt-Audit-Aufzeichnung erstellt, ebenfalls langsamer. Abhängig von der Netzwerkleistung kann das Öffnen von Netzwerkdateien einige Zeit beanspruchen. Die Netzwerkleistung hängt nicht nur mit der physischen Netzwerk-Hardware zusammen, sondern auch mit dem Netzwerk-Traffic und -Design.

Hinweis: Wenn der ClearCore2-Dienst während der Netzwerkerfassung unterbrochen wird, werden die partiellen Probendaten der zu erfassenden Probe zum Zeitpunkt der Unterbrechung nicht in die Datendatei geschrieben.

Hinweis: Wenn Sie eine Netzwerkerfassung in einer regulierten Umgebung verwenden, synchronisieren Sie die Uhrzeit des Computers mit der Uhrzeit des Servers, um genaue Zeitstempel zu erhalten. Die Serverzeit wird für die Erstellungszeit der Datei verwendet. Der „Audit Trail Manager“ zeichnet die Erstellungszeit der Datei über die lokale Computerzeit auf.

VORSICHT: Möglicher Datenverlust. Speichern Sie die Aufzeichnungsdaten mehrerer Erfassungscomputer nicht in derselben Netzwerkdatendatei.

Vorteile der Netzwerkerfassung

Die Datenerfassung im Netzwerk bietet eine sichere Methode, mit Projektordnern zu arbeiten, die sich vollständig auf Netzwerkservern befinden. Dies reduziert die Komplexität beim lokalen Erfassen von Daten und beim anschließenden Verschieben der Daten an einen Netzwerkstandort zur Speicherung. Da Netzlaufwerke normalerweise automatisch gesichert werden, wird außerdem die Notwendigkeit zur Sicherung lokaler Laufwerke reduziert oder eliminiert.

Sicheres Netzwerkkonto

In einer regulierten Umgebung, in der Daten in einem Netzwerkordner erfasst werden, wird dringend empfohlen, dass Benutzer über keine Berechtigungen zum Löschen für den Zielordner verfügen. Ohne Berechtigungen zum Löschen für diesen Ordner kann SCIEX OS jedoch nicht die optimale Leistung erzielen. Über die SNA-Funktion (Secure Network Account, sicheres Netzwerkkonto) wird ein Netzwerkkonto identifiziert, das uneingeschränkte Dateiberechtigungen für das Netzwerk-Stammverzeichnis besitzt. Der ClearCore2-Dienst verwendet dieses Konto zum Übertragen von Daten in den Netzwerkordner.

Das SNA muss über einen Vollzugriff verfügen für:

- Den Netzwerkstammverzeichnis-Ordner
- Den Ordner `SCIEX OS Data\NetworkBackup` auf dem Erfassungscomputer
- Den Ordner `SCIEX OS Data\TempData` auf dem Erfassungscomputer

Folgendes ist für das SNA nicht erforderlich:

- Es muss nicht zur Administratorgruppe auf dem Computer gehören.
- Es muss nicht in der SCIEX OS Benutzerverwaltungsdatenbank vorhanden sein.

Das SNA ist auf der Seite „Projects“ im Arbeitsbereich „Configuration“ festgelegt. Es kann nur ein gültiges Windows Netzwerk oder Domänenkonto angegeben werden.

Wenn kein SNA festgelegt ist, verwendet SCIEX OS die Anmeldedaten des aktuell angemeldeten Benutzers, um die Daten in das Stammverzeichnis des Netzwerks zu übertragen. Damit der Transfer erfolgreich ist, muss das Konto über Schreibzugriff auf alle Projektordner verfügen, in denen Daten erfasst werden, und zwar ungeachtet dessen, welcher Benutzer die Charge zur Erfassung übermittelt hat.

Datentransferprozess

Wenn SCIEX OS Daten in einem Speicherplatz im Netzwerk erfasst, wird jede Probe zunächst in einem Ordner auf dem lokalen Laufwerk gespeichert und dann in das Netzwerk übertragen. Wenn der erfolgreiche Transfer der gesamten Datendatei bestätigt wurde, wird der lokale Ordner, der die Daten enthält, gelöscht. Sollte das Netzwerk während des Prozesses nicht mehr verfügbar sein, versucht SCIEX OS es alle 15 Minuten erneut, bis der Transfer erfolgreich ist.

Informationen über den Datenzugriff während einer längeren Unterbrechung der Netzwerkverbindung finden Sie im Abschnitt: Entfernen von Proben aus einem Netzwerktransfer-Ordner.

Konfigurieren der Netzwerkerfassung

Ein Stammverzeichnis ist der Ordner, in dem SCIEX OS Daten speichert. Um sicher zu gehen, dass Projektinformationen sicher gespeichert werden, erstellen Sie das Stammverzeichnis mithilfe von SCIEX OS. Erstellen Sie keine Projekte in Windows-Explorer.

Wenn Sie, optional, Stammverzeichnisse in einer Netzwerkressource erstellen, legen Sie die „**Credentials for Secure Network Account**“ fest. Es handelt sich hierbei um das in der Netzwerkressource definierte sichere Netzwerkkonto. Siehe Abschnitt: Sicheres Netzwerkkonto.

Informationen zum Erstellen von Projekten und Teilprojekten finden Sie im Dokument: *SCIEX OS-Software-Benutzerhandbuch*.

Spezifizieren eines sicheren Netzwerkkontos

Wenn Projekte in einer Netzwerkressource gespeichert werden, kann ein sicheres Netzwerkkonto spezifiziert werden, um sicherzustellen, dass alle Benutzer der Workstation über den erforderlichen Zugriff auf die Netzwerkressource verfügen.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Projects**.
3. Klicken Sie im Abschnitt **Advanced** auf **Credentials for Secure Network Account**.
4. Geben Sie den Benutzernamen, das Passwort und die Domäne für das in der Netzwerkressource definierte sichere Netzwerkkonto ein.
5. Klicken Sie auf **OK**.

Auditing 7

In diesem Abschnitt wird die Verwendung der Auditing-Funktion beschrieben. Informationen über Windows-Auditing-Funktionen finden Sie im Abschnitt: System-Audits .

Audit-Trails

Geprüfte Ereignisse werden in Audit Trails gespeichert. Es sind zwei Arten von Audit Trails verfügbar: Workstation und Projekt.

Workstation-Audit-Trails sind Dateien, die die geprüften Ereignisse für den Computer speichern, auf dem SCIEX OS oder die Central Administrator Console (CAC) Software ausgeführt wird. Eine vollständige Liste der geprüften Ereignisse finden Sie im Abschnitt: Workstation-Audit-Trail.

Ein Projekt-Audit-Trail ist die Datei, die die geprüften Ereignisse für das Projekt speichert. Eine vollständige Liste der geprüften Ereignisse finden Sie im Abschnitt: Projekt-Audit-Trail. In SCIEX OS und in der CAC Software zeigt der Arbeitsbereich „Audit Trail“ die Audit Trails für die Projekte im aktuellen Stammverzeichnis an. Verarbeitungs-Audit-Trail-Ereignisse sind in der Projekt-Audit-Trail-Map enthalten und werden gemeinsam mit der „Results Table“ gespeichert.

Audit-Trails bilden in Verbindung mit Dateien, wie z. B. .wiff2- und „Results Table“-Dateien, gültige elektronische Aufzeichnungen, die für Compliance-Zwecke verwendet werden können.

Tabelle 7-1: -Audit-Trails

Audit-Trail	Beispiele für aufgezeichnete Ereignisse	Verfügbare Audit-Maps (Speicherort)	Standard-Audit-Maps

Workstation (SCIEX OS)	• Änderungen an:
	  • Zuweisung der aktiven Audit-Map
	  • Geräte-Tuning
	  • Probenwartesc hlangen
	  • Sicherheit
	  • Tuning
	  • Geräte
		• Ordner `C:\ProgramData\SCIEX\Audit Data`	• No Audit Map

Tabelle 7-1: -Audit-Trails (Fortsetzung)

Audit-Trail	Beispiele für aufgezeichnete Ereignisse	Verfügbare Audit-Maps (Speicherort)	Standard-Audit-Maps

Workstation (CAC)	• Änderungen an:
	  • Audit-Map
	  • CAC-Server
	  • Sicherheit
	  • Benutzerprotokoll
		• Ordner `C:\ProgramData\SCIEX\Audit Data`	• Silent Audit Map

Projekt (1x pro Projekt)	• Änderungen an:
	  • Zuweisung der aktiven Audit-Map (SCIEX OS)
	  • Projekt
	  • Daten
	• Drucken
		• Ordner `<project>\Audit Data`	• Spezifiziert auf der Seite „Audit Maps“ des Arbeitsbereichs „Configuration“

Sobald der Workstation-Audit-Trail oder Projekt-Audit-Trail 20.000 Audit-Aufzeichnungen enthält, archivieren SCIEX OS und die CAC Software diese Aufzeichnungen automatisch und beginnen einen neuen Audit-Trail. Weitere Informationen finden Sie im Abschnitt: Audit-Trail-Archive.

Audit-Maps

Eine Audit-Map ist eine Datei, die eine Liste aller Ereignisse enthält, die geprüft werden können sowie Informationen dazu, ob ein Änderungsgrund oder eine elektronische Signatur für das Ereignis erforderlich ist. Es sind zwei Arten von Audit-Maps verfügbar: Workstation und Projekt.

Workstation Audit Maps steuern die Ereignisse, die auf einer Workstation geprüft werden.

Project Audit Maps steuern die Ereignisse, die für ein Projekt geprüft werden und im Projektordner gespeichert werden.

Hinweis: Die Audit-Map für ein Projekt kann in SCIEX OS oder der Central Administrator Console (CAC) Software bearbeitet werden.

Der Benutzer kann viele Workstation- und Projekt-Audit-Maps erstellen. Für jede Workstation und jedes Projekt kann jedoch zeitgleich immer nur eine Audit-Map verwendet werden.

Die für eine Workstation oder ein Projekt verwendete Audit-Map wird als aktive Audit-Map bezeichnet.

Wenn SCIEX OS installiert ist, dann ist die Standard-Audit-Map für alle neuen Projekte „Keine Audit-Map“. Wenn die CAC Software installiert ist, dann ist die Standard-Audit-Map für alle neuen Projekte „Silent Audit-Map“.Der Benutzer kann eine andere aktive Audit-Map als Standard für alle neuen Projekte angeben. Siehe Abschnitt: Ändern einer aktiven Audit-Map für ein Projekt.

Einrichten von Audit-Maps

Bevor Sie mit zu auditierenden Projekten arbeiten können, müssen Sie den Standardarbeitsanweisungen entsprechende Audit-Maps konfigurieren. Es stehen nach der Installation der Software zwar mehrere standardmäßige Audit-Map-Vorlagen zur Verfügung, Sie müssen jedoch möglicherweise eine benutzerdefinierte Map erstellen. Stellen Sie sicher, dass Sie eine geeignete Audit-Map für den Workstation-Audit-Trail und eine geeignete Audit-Map für die einzelnen Projekte haben.

Tabelle 7-2: Checkliste für das Konfigurieren von Auditing

Aufgabe	Siehe
Erstellen einer Audit-Map für den Workstation-Audit-Trail	• Erstellen einer Workstation-Audit-Map. • Bearbeiten einer Workstation-Audit-Map.
Anwendung der Audit-Map auf den Workstation-Audit-Trail	• Ändern einer aktiven Audit-Map für eine Workstation.
Erstellen einer standardmäßig aktiven Audit-Map für neue Projekte	• Erstellen einer Projekt-Audit-Map.
Konfiguration der Audit-Map, die für bestehende Projekte verwenden werden soll	• Erstellen einer Projekt-Audit-Map. • Bearbeiten einer Projekt-Audit-Map.
Anwendung der Audit-Map auf bestehende Projekte	• Ändern einer aktiven Audit-Map für ein Projekt.

Installierte Audit-Map-Vorlagen

Die Software umfasst mehrere Audit-Map-Vorlagen. Diese Vorlagen können nicht bearbeitet oder gelöscht werden.

Tabelle 7-3: Installierte Audit-Maps

Audit-Map	Beschreibung
Example Audit Map	Ausgewählte Ereignisse werden geprüft. Nur zu Darstellungszwecken.
Full Audit Map	Alle Ereignisse werden geprüft. Für alle Ereignisse sind elektronische Signaturen und Gründe erforderlich.

Tabelle 7-3: Installierte Audit-Maps (Fortsetzung)

Audit-Map	Beschreibung
No Audit Map	Es werden keine Ereignisse überprüft. **Hinweis:** Das Ereignis **Change Active Audit Map Assignment** wird immer aufgezeichnet, auch wenn die Vorlage „No Audit Map“ verwendet wird.
Silent Audit Map	Alle Ereignisse werden geprüft. Für kein Ereignis werden elektronische Signaturen und Gründe verlangt.

Für Beschreibungen der Audit-Trail-Arten und ihrer Beziehungen zu Audit-Maps siehe die Tabelle: Tabelle 7-1. Für Informationen über die in Audit-Trails erfassten Ereignisse siehe Abschnitt: Audit-Trail-Aufzeichnungen.

Für Informationen über den Prüfprozess siehe die Tabelle: Tabelle 7-2.

Arbeiten mit Audit-Maps

Die Software umfasst mehrere installierte Audit-Map-Vorlagen. Für Beschreibungen der Audit-Map-Vorlagen siehe Abschnitt: Installierte Audit-Map-Vorlagen. Für eine Checkliste der empfohlenen Schritte beim Einrichten von Audits siehe Abschnitt: Einrichten von Audit-Maps.

Wenn eine aktive Audit-Map-Vorlage in der Software oder im Datei-Explorer gelöscht wird, dann verwendet ein Projekt, das diese Audit-Map-Vorlage verwendet, stattdessen die Silent-Audit-Map.

Projekt-Audit-Maps

Projekt-Audit-Maps steuern die Auditierung von Projektereignissen. Für eine Liste auditierbarer Projektereignisse siehe Abschnitt: Projekt-Audit-Trail.

Erstellen einer Projekt-Audit-Map

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Project Templates“.
4. Wählen Sie im Feld **Edit map template** eine Vorlage als Grundlage für die neue Map aus.
5. Klicken Sie auf **Add Template** ( ).
   Das Dialogfeld „Add a Project Audit Map Template“ wird geöffnet.
6. Geben Sie den Namen der neuen Map ein und klicken Sie dann auf **OK**.
7. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:

a. Markieren Sie das Kontrollkästchen **Audited** für das Ereignis.

b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Reason Required** aus.

c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig Required** aus.

d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Use Predefined Reason Only** aus und definieren Sie die Gründe.

8. Achten Sie darauf, dass das Kontrollkästchen **Audited** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
9. Klicken Sie auf **Save Template**.
   Das System fragt, ob die neue Map auf Projekte angewendet werden soll.
10. Führen Sie einen der folgenden Schritte aus:

    - Um die neue Map auf Projekte anzuwenden, klicken Sie auf **Yes**, wählen Sie die Projekte für die neue Map aus und klicken Sie dann auf **Apply**.
    - Wenn die neue Map nicht auf vorhandene Projekte angewendet werden soll, klicken Sie auf **No**.

11. (Optional) Klicken Sie auf **Use as Default for New Projects**, um diese Audit Map als Standard für alle neuen Projekte zu verwenden.

Bearbeiten einer Projekt-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht bearbeitet werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Project Templates“.
4. Wählen Sie im Feld **Edit map template** die zu ändernde Map aus.
5. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:

   a. Markieren Sie das Kontrollkästchen **Audited** für das Ereignis.

   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Reason Required** aus.

   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig Required** aus.

   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Use Predefined Reason Only** aus und definieren Sie die Gründe.

6. Achten Sie darauf, dass das Kontrollkästchen **Audited** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
7. Klicken Sie auf **Save Template**.
   Das System fragt, ob die neue Map auf Projekte angewendet werden soll.
8. Führen Sie einen der folgenden Schritte aus:

- Um die neue Map auf Projekte anzuwenden, klicken Sie auf **Yes**, wählen Sie die Projekte für die neue Map aus und klicken Sie dann auf **Apply**.
- Wenn die neue Map nicht auf vorhandene Projekte angewendet werden soll, klicken Sie auf **No**.

Ändern einer aktiven Audit-Map für ein Projekt

Wenn eine Audit-Map für ein Projekt angewendet wird, ist sie eine aktive Audit-Map. Die Audit-Konfiguration in der aktiven Audit-Map bestimmt, welche Ereignisse in den Audit-Trails aufgezeichnet werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Project Templates“.
4. Wählen Sie im Feld **Edit map template** die Audit-Map aus, die dem Projekt zugewiesen werden soll.
5. Klicken Sie auf **Apply to Existing Projects**.
   Das Dialogfeld „Apply Project Audit Map Template“ wird geöffnet.
6. Aktivieren Sie die Kontrollkästchen für die Projekte, auf die diese Audit-Map angewendet werden soll.
7. Klicken Sie auf **Apply**.

Löschen einer Projekt-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht gelöscht werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Project Templates“.
4. Wählen Sie im Feld **Edit map template** die zu löschende Map aus.
5. Klicken Sie auf **Delete Template**.
   Das System fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **Yes**.

Workstation-Audit-Maps

Workstation-Audit-Maps steuern die Auditierung von Workstation-Ereignissen. Für eine Liste auditierbarer Workstation-Ereignisse siehe Abschnitt: Workstation-Audit-Trail.

Erstellen einer Workstation-Audit-Map

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Workstation Templates“.

4. Wählen Sie im Feld **Edit map template** eine Vorlage als Grundlage für die neue Map aus.
5. Klicken Sie auf **Add Template** ().
   Das Dialogfeld „Add a Workstation Audit Map Template“ wird geöffnet.
6. Geben Sie den Namen der neuen Map ein und klicken Sie dann auf **OK**.
7. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Audited** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Reason Required** aus.
   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig Required** aus.
   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Use Predefined Reason Only** aus und definieren Sie die Gründe.
8. Achten Sie darauf, dass das Kontrollkästchen **Audited** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
9. Klicken Sie auf **Save Template**.
10. (Optional) Klicken Sie auf **Apply to the Workstation**, um die Audit-Map als aktive Audit-Map für die Workstation zu verwenden.

Bearbeiten einer Workstation-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht bearbeitet werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Workstation Templates“.
4. Wählen Sie im Feld **Edit map template** die zu ändernde Map aus.
5. Für die Auswahl und Konfiguration der aufzuzeichnenden Ereignisse gehen Sie wie folgt vor:
   a. Markieren Sie das Kontrollkästchen **Audited** für das Ereignis.
   b. (Optional) Wenn ein Grund erforderlich ist, wählen Sie **Reason Required** aus.
   c. (Optional) Wenn eine elektronische Signatur erforderlich ist, wählen Sie **E-Sig Required** aus.
   d. (Optional) Wenn vordefinierte Gründe erforderlich sind, wählen Sie **Use Predefined Reason Only** aus und definieren Sie die Gründe.
6. Achten Sie darauf, dass das Kontrollkästchen **Audited** für Ereignisse, die nicht protokolliert werden sollen, frei bleibt.
7. Klicken Sie auf **Save Template**.

8. (Optional) Klicken Sie auf **Apply to the Workstation**, um die Audit-Map als aktive Map für die Workstation zu verwenden.

Ändern einer aktiven Audit-Map für eine Workstation

Wenn eine Audit-Map für eine Workstation angewendet wird, ist sie eine aktive Audit-Map. Die Audit-Konfiguration in der aktiven Audit-Map bestimmt, welche Ereignisse in den Audit-Trails aufgezeichnet werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Workstation Templates“.
4. Wählen Sie im Feld **Edit map template** die Map aus, die auf die Workstation angewendet werden soll.
5. Klicken Sie auf **Apply to the Workstation**.

Löschen einer Workstation-Audit-Map

Hinweis: Installierte Audit-Map-Vorlagen können nicht gelöscht werden.

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Audit Maps**.
3. Öffnen Sie die Registerkarte „Workstation Templates“.
4. Wählen Sie im Feld **Edit map template** die zu löschende Map aus.
5. Klicken Sie auf **Delete Template**.
   Das System fordert Sie zur Bestätigung auf.
6. Klicken Sie auf **Yes**.

Anzeigen, Durchsuchen, Exportieren und Drucken von Audit Trails

Dieser Abschnitt enthält Informationen über das Anzeigen von Audit Trails und archivierten Audit Trails. Er enthält auch Anweisungen zum Exportieren, Drucken, Durchsuchen und Sortieren von Audit-Aufzeichnungen innerhalb von Audit Trails.

Anzeigen eines Audit-Trails

1. Öffnen Sie den Arbeitsbereich „Audit Trail“.
2. Wählen Sie den anzuzeigenden Audit-Trail aus:
   - Wenn Sie einen Audit-Trail anzeigen möchten, klicken Sie auf **Workstation**.
   - Wenn Sie einen Projekt-Audit-Trail anzeigen möchten, wählen Sie das Projekt aus.
3. Wenn Sie die Details einer Audit-Aufzeichnung anzeigen möchten, wählen Sie die Aufzeichnung aus.

Durchsuchen oder Filtern von Audit-Aufzeichnungen

1. Öffnen Sie den Arbeitsbereich „Audit Trail“.
2. Wählen Sie den zu durchsuchenden Audit-Trail aus.
3. Um nach bestimmten Auditdatensätzen zu suchen, geben Sie Text in das Feld **Find in Page** ein.
   Alle Suchergebnisse für den eingegebenen Text auf der Seite werden hervorgehoben.
4. Um die Audit-Trail-Aufzeichnungen zu filtern, gehen Sie wie folgt vor:
   a. Klicken Sie auf das Filter-Symbol (Trichter).
      Das Dialogfeld Filter Audit Trail wird geöffnet.
   b. Geben Sie die Filterkriterien ein.
   c. Klicken Sie auf **OK**.

Anzeigen eines archivierten Audit-Trails

Sobald ein Audit-Trail 20.000 Audit-Aufzeichnungen enthält, archiviert SCIEX OS diese Aufzeichnungen automatisch und beginnt einen neuen Audit-Trail. Die Audit-Trail-Dateien werden unter einem Namen archiviert, der den Typ des Audit-Trails und das Datum und die Uhrzeit angibt. Beispiel: Der Dateiname für ein Workstation-Audit-Trail-Archiv hat das Format „WorkstationAuditTrailData-<Workstation-Name>-<JJJJ><MMTTHHMMSS>.atds“.

Dieses Verfahren kann auch verwendet werden, um einen Audit-Trail für eine Ergebnistabelle zu öffnen.

1. Öffnen Sie den Arbeitsbereich „Audit Trail“.
2. Klicken Sie auf **Browse**.
3. Navigieren Sie zu dem zu öffnenden archivierten Audit-Trail, wählen Sie ihn aus und klicken Sie dann auf **OK**.

Hinweis: Um den Audit-Trail für eine Ergebnistabelle zu öffnen, öffnen Sie die zugehörige qsession-Datei.

Drucken eines Audit-Trails

1. Öffnen Sie den Arbeitsbereich „Audit Trail“.
2. Wählen Sie den zu druckenden Audit-Trail aus.
3. Klicken Sie auf **Print**.
   Das Dialogfeld Print wird geöffnet.
4. Wählen Sie den Drucker aus und klicken Sie dann auf **OK**.

Exportieren von Audit-Trail-Aufzeichnungen

1. Öffnen Sie den Arbeitsbereich „Audit Trail“.
2. Wählen Sie den zu exportierenden Audit-Trail aus.

3. Klicken Sie auf **Export**.
4. Navigieren Sie zu dem Speicherort der exportierten Datei, geben Sie einen **File name** ein und klicken Sie auf **Save**.
   Der Audit-Trail wird als CSV-Datei gespeichert.

Audit-Trail-Aufzeichnungen

Dieser Abschnitt beschreibt die Felder in den Audit-Trail-Aufzeichnungen.

Bei den Workstation- und Projekt-Audit-Trails handelt es sich um verschlüsselte Dateien.

Hinweis: Workstation-Audit-Trails und Archive werden im Ordner `Program Data\SCIEX\Audit Data` gespeichert. Projekt-Audit-Trails und Archive werden im Ordner `Audit Data` für das Projekt gespeichert.

Tabelle 7-4: Felder der Ereignisaufzeichnung

Feld	Beschreibung
Timestamp	Datum und Uhrzeit der Aufzeichnung.
Event Name	Das Modul, das das Ereignis erzeugt hat.
Description	Eine Beschreibung des Ereignisses.
Reason	Der Grund für die Änderung, wie vom Benutzer angegeben (falls erforderlich).
E-signature	Angabe, ob eine elektronische Signatur bereitgestellt wurde.
Full User Name	Der Name des Benutzers.
User	Der User Principal Name (UPN) des Benutzers.
Category	Die Art des Ereignisses.

Für Listen aller Ereignisse, die in den Workstation- und Projekt-Audit-Trails aufgezeichnet werden, siehe die Abschnitte: Workstation-Audit-Trail und Projekt-Audit-Trail.

Audit-Trail-Archive

Audit-Aufzeichnungen sammeln sich im Projekt-Audit-Trail und im Workstation-Audit-Trail an. Die resultierenden Dateien können sehr groß werden und daher schwierig zu navigieren und zu verwalten sein.

Wenn ein Audit-Trail 20.000 Aufzeichnungen erreicht, wird er archiviert. Dem Audit-Trail wird eine letzte Archivaufzeichnung hinzugefügt. Sie wird unter einem Namen bestehend aus der Art des Audit-Trails, dem Datum und der Uhrzeit gespeichert. Es wird ein neuer Audit-Trail erstellt. Die erste Aufzeichnung im neuen Audit-Trail gibt an, dass der Audit-Trail archiviert wurde. Ebenfalls enthalten ist der Pfad zu dem archivierten Audit-Trail.

Archive für Workstation-Audit-Trails werden im Ordner `C:\ProgramData\SCIEX\Audit Data` gespeichert. Die Dateinamen sind im Format WorkstationAuditTrailData-<*workstation*

name>-<*YYYY*><*MMDDHHMMSS*>.atds. Beispiel: `WorkstationAuditTrailData-SWDSXPT158-20190101130401.atds`.

Archive für Projekt-Audit-Trails werden im Ordner `Audit Data` für das Projekt gespeichert.

Zugriff auf Daten während Netzwerkunterbrechungen A

Lokale Anzeige und Verarbeitung von Daten

Wenn während einer Netzwerkerfassung eine vorübergehende Netzwerkunterbrechung auftritt, können Sie auf dem Erfassungscomputer über den Ordner `NetworkBackup` auf die erfassten Daten zugreifen. Um die Beschädigung der Daten zu vermeiden, empfehlen wir dringend, die Datendateien aus dem `NetworkBackup`-Ordner an einen neuen Speicherort zu kopieren, bevor diese angezeigt oder verarbeitet werden. Die ursprünglichen Dateien sollten im Ordner `NetworkBackup` verbleiben.

SCIEX OS überprüft alle 15 Minuten, ob der Speicherplatz im Netzwerk verfügbar ist. Wenn dies der Fall ist, wird der Datentransfer fortgesetzt.

Der Ordner `NetworkBackup` wird in der Regel im lokalen Stammverzeichnis `D:\SCIEX OS Data\NetworkBackup` gespeichert. Die Datendateien für die einzelnen Chargen werden in einem Ordner gespeichert, der mit einer eindeutigen Kennzeichnung benannt ist. Der Datums- und Zeitstempel der Ordner gibt das Startdatum und die Startzeit der Charge an und kann Aufschluss darüber geben, welcher Ordner die gesuchten Daten enthält.

Entfernen von Proben aus einem Netzwerktransfer-Ordner

Wenn die Netzwerkverbindung für längere Zeit unterbrochen wird oder wenn das Stammverzeichnis des Netzwerks geändert wird, ist es möglicherweise erforderlich, Datendateien aus dem Ordner für den Netzwerktransfer zu entfernen. Wir empfehlen, diese Aktion von einem erfahrenen Systemadministrator mit fundierten technischen Netzwerkkenntnissen durchführen zu lassen.

1. Öffnen Sie den Arbeitsbereich Queue.
2. Stoppen Sie die Warteschlange.
3. Brechen Sie alle verbleibenden Proben in der Charge ab, die die zu entfernenden Proben enthält.
4. Schließen Sie SCIEX OS.
5. Stoppen Sie **Clearcore2.Service.exe**.

   Tipp! Führen Sie diese Aufgabe im Windows Service Manager aus.

6. Verschieben Sie alle Dateien und Ordner in den Ordnern `OutBox` und `NetworkBackup`, die auf den Transfer in das nicht verfügbare Stammverzeichnis warten, vorübergehend in einen anderen Ordner. Löschen Sie nicht die Ordner `OutBox` oder `NetworkBackup`.

Hinweis: Der Ordner `OutBox` ist ein verborgener Ordner, der sich in der Regel im lokalen Stammverzeichnis `D:\SCIEX OS Data\TempData\Outbox` befindet. Wenn die Dateien und Ordner in `Outbox` nicht mehr benötigt werden, können Sie entfernt werden.

VORSICHT: Möglicher Datenverlust. Löschen Sie die Datei nicht, wenn die Daten der festsitzenden Probe erhalten bleiben müssen.

7. Starten Sie SCIEX OS.
   Innerhalb von 15 Minuten versucht SCIEX OS, eine Verbindung zur Netzwerkressource herzustellen. Wenn die Verbindung erfolgreich ist, wird der Transfer fortgesetzt. Wenn der Transfer abgeschlossen ist, werden die Ordner aus dem Ordner `NetworkBackup` gelöscht.

Audit-Ereignisse B

In diesem Abschnitt werden die Audit-Ereignisse in SCIEX OS aufgelistet. Es werden außerdem die entsprechenden Audit-Ereignisse in der Analyst Software aufgelistet für Benutzer, die eine Migration von der Analyst Software zu SCIEX OS durchführen.

Projekt-Audit-Trail

Jedes Projekt hat einen Projekt-Audit-Trail. Der Projekt-Audit-Trail wird im Ordner „`Audit Data`“ für das Projekt gespeichert. Der Name der Audit-Trail-Datei ist „`ProjectAuditEvents.atds`“.

Hinweis: Die Standard-Audit-Map für neue Projekte, die in der Central Administrator Console (CAC) Software erstellt wurden, ist die **Silent Audit Map**.

Ereignisse des Projekt-Audit-Trails werden sowohl in der CAC Software als auch in SCIEX OS angezeigt.

Tabelle B-1: Ereignisse des Projekt-Audit-Trails

SCIEX OS oder CAC	Analyst Software
Arbeitsbereich „Analytics“	
Actual Concentration changed	Quantifizierungsereignisse: ‚Concentration‘ wurde geändert
Auto-Processing File saved	—
Barcode ID changed	—
Comparison sample changed in non-targeted workflow	—
Custom columns modified	Quantifizierungsereignisse: ‚Custom Title‘ wurde geändert
Data exploration opened	Projektereignisse: Datendatei wurde geöffnet
Data exported	—
Data transferred to LIMS	—
Dilution Factor changed	Quantifizierungsereignisse: ‚Dilution Factor‘ wurde geändert
External calibration changed	—
External calibration exported	—

Tabelle B-1: Ereignisse des Projekt-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
File saved	Projektereignisse: „Results Table“ für die Quantifizierung wurde erstellt, „Results Table“ für die Quantifizierung wurde geändert, Quantifizierungsereignisse: „Results Table“ wurde gespeichert
Formula column changed	Quantifizierungsereignisse: Formelname wurde geändert, Formelname wurde hinzugefügt, Formel-String wurde geändert, Formelspalte wurde entfernt
Integration cleared	—
Integration parameters changed	Quantifizierungsereignisse: Quantifizierungspeak wurde integriert
Library search result changed	—
Manual Integration	Quantifizierungsereignisse: Quantifizierungspeak wurde integriert
Manual Integration reverted	Quantifizierungsereignisse: Quantifizierungspeak wurde wieder auf den ursprünglichen Peak zurückgesetzt
MS/MS selection changed	—
Processing method changed and applied	Quantifizierungsereignisse: Quantifizierungsmethode wurde geändert
Report created	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Results Table approved	Quantifizierungsereignisse: Qualitätssicherungsprüfer hat auf eine „Results Table“ zugegriffen
Results Table created	Quantifizierungsereignisse: „Results Table“ wurde erstellt
Results Table locked	—
Results Table unlocked	—
Sample ID changed	Quantifizierungsereignisse: ‚Sample ID‘ wurde geändert
Sample Name changed	Quantifizierungsereignisse: ‚Sample Name‘ wurde geändert

Tabelle B-1: Ereignisse des Projekt-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Samples added or removed	Quantifizierungsereignisse: Dateien wurden zur „Results Table“ hinzugefügt, Dateien wurden aus der „Results Table“ entfernt, Proben wurden hinzugefügt/entfernt
Sample Type changed	Quantifizierungsereignisse: ‚Sample Type‘ wurde geändert
Std. Addition Actual concentration changed	—
Used column selection changed	Quantifizierungsereignisse: ‚Use It‘ wurde geändert
Window/pane printed	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Seite „Audit Map“	
Project Audit Map changed	Projektereignisse: Projekteinstellungen wurden geändert
Project Audit Trail Printed	—
Project Audit Trail Exported	—
Arbeitsbereich „Batch“	
Batch information imported from LIMS/ text	—
Print	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Arbeitsbereich „Explorer“	
Open Sample(s)	Projektereignisse: Datendatei wurde geöffnet
Recalibrate sample(s)	—
Recalibrate sample(s) started	—
Arbeitsbereich „LC Method“	
Print	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Arbeitsbereich „MS Method“	

Tabelle B-1: Ereignisse des Projekt-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Print	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Arbeitsbereich „Queue“	
Sample Transferred	—

Workstation-Audit-Trail

Jede Workstation hat einen Workstation-Audit-Trail. Der Workstation-Audit-Trail wird im Ordner „`Program Data\SCIEX\Audit Data`“ gespeichert. Der Name der Audit-Trail-Datei besitzt das Format: `WorkstationAuditTrailData.atds`.

Hinweis: Die Standard-Audit-Map für neue Workstations in der Central Administrator Console (CAC) Software ist die **Silent Audit Map**.

Ereignisse des Workstation-Audit-Trails werden sowohl in der CAC Software als auch in SCIEX OS angezeigt.

Tabelle B-2: Ereignisse des Workstation-Audit-Trails

SCIEX OS oder CAC	Analyst Software
Instrument Tune (SCIEX OS)	
Firmware changed	—
Manual Tuning	Instrumentenereignisse: Tune-Parameter-Einstellungen geändert
Automatic Tuning	Instrumentenereignisse: Tune-Parameter-Einstellungen geändert
Print Procedure Result in MS Tune	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Hardware Configuration (SCIEX OS)	
Devices Activated	Instrumentenereignisse: Hardwareprofil wurde aktiviert
Devices Deactivated	Instrumentenereignisse: Hardwareprofil wurde deaktiviert
Data File Checksum (SCIEX OS)	
Wiff data file checksum has been changed	—

Tabelle B-2: Ereignisse des Workstation-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Arbeitsbereich „Explorer“ (SCIEX OS)	
Open Sample(s)	Projektereignisse: Datendatei wurde geöffnet
Recalibrate samples(s)	—
Recalibrate samples(s) started	—
Seite „Audit Map“[1]	
Workstation Audit Map changed	Instrumentenereignisse: Instrumenteneinstellungen wurden geändert
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	—
Arbeitsbereich „Queue“ (SCIEX OS)	
Sample moved in Queue	Instrumentenereignisse: Probe wurde in der Chargendatei von Position x zu Position y verschoben
Batch moved in Queue	Instrumentenereignisse: Charge verschieben
Reaquiring sample	Instrumentenereignisse: Probe(n) neu erfassen
Sample starts to acquire	—

[1] Diese Ereignisse werden sowohl in SCIEX OS als auch in CAC aufgezeichnet.

Tabelle B-2: Ereignisse des Workstation-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
Print Queue	Projektereignisse: Dokument wird auf Drucker gedruckt, Druckvorgang für Dokument auf Drucker beendet
Sample acquistion has completed	Projektereignisse: Probe wurde zur Datendatei hinzugefügt
Automatic reinjections Occurred	—
Automatic injection Occurred	—
Sicherheit[1]	
Auto logoff by system	Instrumentenereignisse: Benutzer hat sich abgemeldet
Forced logoff by another user	Instrumentenereignisse: Benutzer hat sich abgemeldet
Forced Logoff failed	—
Screen unlock failed	—
Secure Network Account credentials have been changed	Instrumentenereignisse: Erfassungskonto wurde geändert
Secure Network Account credentials have been removed	Instrumentenereignisse: Erfassungskonto wurde geändert
Secure Network Account credentials have been specified	Instrumentenereignisse: Erfassungskonto wurde geändert
Security configuration changed	Instrumentenereignisse: Die Sicherheitskonfiguration wurde geändert, Bildschirmsperre wurde geändert, Automatisches Abmelden wurde geändert
User added/deleted	Instrumentenereignisse: Benutzer wurde hinzugefügt, Benutzer wurde gelöscht
User has logged in	Instrumentenereignisse: Benutzer hat sich angemeldet
User has logged out	Instrumentenereignisse: Benutzer hat sich abgemeldet
User has turned off exclusive mode	—
User Login Failed	Instrumentenereignisse: Benutzeranmeldung ist fehlgeschlagen
User management settings have been exported	—

Tabelle B-2: Ereignisse des Workstation-Audit-Trails (Fortsetzung)

SCIEX OS oder CAC	Analyst Software
User management settings have been imported	—
User management settings have been restored	—
User role assigned to user/user group	Instrumentenereignisse: Benutzer hat Benutzertyp geändert
User role deleted	Instrumentenereignisse: Benutzertyp wurde gelöscht
User role modified	Instrumentenereignisse: Benutzertyp wurde geändert
UserLog[1]	
Print Event Log	—

Zuordnung von Berechtigunen zwischen SCIEX OS und der Analyst Software

C

Dieser Abschnitt ist für Benutzer, die eine Migration von der Analyst Software zu SCIEX OS durchführen, um ihnen dabei zu helfen, ihre Benutzersicherheitseinstellungen zu migrieren. Es werden die Berechtigungen für die Analyst Software angezeigt, die den Berechtigungen für SCIEX OS entsprechen.

Tabelle C-1: Zuordnung von Berechtigungen

SCIEX OS	Analyst Software
Arbeitsbereich „Batch“	
Submit unlocked methods	—
Open	Charge: Vorhandene Chargen öffnen
Save as	Charge: Neue Chargen erstellen, Importieren, Chargen bearbeiten, Chargen speichern, Chargen überschreiben
Submit	Charge: Chargen übergeben
Save	Charge: Chargen speichern, Chargen überschreiben
Save ion reference table	—
Add data sub-folders	—
Configure Decision Rules	—
Arbeitsbereich „Configuration“	
General tab	—
General: change regional setting	—
General: full screen mode	—
General: Stop Windows services	—
LIMS Communication tab	—
Audit maps tab	Audit Trail Manager: Audit-Trail-Einstellungen ändern, Audit-Maps erstellen oder ändern
Queue tab	—
Queue: instrument idle time	—

Tabelle C-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS	Analyst Software
Queue: max. number of acquired samples	—
Queue: other queue settings	—
Projects tab	—
Projects: create project	Analyst-Anwendung: Projekt erstellen
Projects: apply an audit map template to an existing project	Audit Trail Manager: Audit-Trail-Einstellungen ändern
Projects: create root directory	Analyst-Anwendung: Stammverzeichnis erstellen
Project: set current root directory	Analyst-Anwendung: Stammverzeichnis festlegen
Projects: specify network credentials	—
Projects: Enable checksum writing for wiff data creation	—
Projects: clear root directory	—
Devices tab	Hardwarekonfiguration: Erstellen, Löschen, Bearbeiten, Aktivieren/Deaktivieren
User management tab	Sicherheitskonfiguration
Force user logoff	Anwendung entsperren/abmelden
Arbeitsbereich „Event Log“	
Access event log workspace	—
Archive log	—
Arbeitsbereich „Audit Trail“	
Access audit trail workspace	Audit Trail Manager: Audit-Trail-Daten anzeigen
View active audit map	Audit Trail Manager: Audit-Trail-Daten anzeigen
Print/Export audit trail	Audit Trail Manager: Audit-Trail-Daten anzeigen
Feld „Data Acquisition“	
Start	—
Stop	—
Save	—
Arbeitsbereiche „MS Method“ und „LC Method“	

Tabelle C-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS	Analyst Software
Access method workspace	—
New	Erfassungsmethode: Erfassungsmethode erstellen/speichern
Open	Erfassungsmethode: Erfassungsmethode schreibgeschützt öffnen (Erfassungsmodus)
Save	Erfassungsmethode: Erfassungsmethoden überschreiben, Erfassungsmethode erstellen/speichern
Save as	Erfassungsmethode: Erfassungsmethoden überschreiben, Erfassungsmethode erstellen/speichern
Lock/Unlock method	—
Arbeitsbereich „Queue“	
Manage	Proben-Warteschlange: Neu erfassen, Probe oder Charge Löschen, Charge verschieben
Start/Stop	Proben-Warteschlange: Probe starten, Probe stoppen, Probe abbrechen, Warteschlange anhalten
Print	Berichtsvorlagen-Editor: Drucken
Arbeitsbereich „Library“	
Access library workspace	Durchsuchen: Speicherort der Bibliothek einrichten, Benutzeroptionen der Bibliothek einrichten, Bibliothek-Datensatz hinzufügen, Spektrum zur Bibliothek hinzufügen, Bibliothek-Datensatz ändern (überschreibt „hinzufügen/löschen“, falls deaktiviert), MS-Spektrum löschen, UV-Spektrum löschen, Struktur löschen, Bibliothek anzeigen, Bibliothek durchsuchen
CAC settings	
Enable Central Administration	—
Arbeitsbereich „MS Tune“	
Access MS Tune workspace	—
Advanced MS tuning	Abstimmen: Instrumentenoptimierung, Manuelles Tuning, Tuning-Optionen bearbeiten

Tabelle C-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS	Analyst Software
Advanced troubleshooting	—
Quick status check	Abstimmen: Instrumentenoptimierung
Restore instrument data	Abstimmen: Tuning-Optionen bearbeiten, Instrumentendaten bearbeiten
Arbeitsbereich „Explorer“	
Access explorer workspace	—
Export	Durchsuchen: Daten in Textdatei speichern
Print	Berichtsvorlagen-Editor: Drucken
Options	—
Recalibrate	Abstimmen: Aus aktuellem Spektrum kalibrieren
Arbeitsbereich „Analytics“	
New results	Quantifizierung: Neue Ergebnistabellen erstellen
Create processing method	Quantifizierung: Quantifizierungsmethoden erstellen
Modify processing method	Quantifizierung: Vorhandene Methoden ändern
Allow Export and Create Report of unlocked Results Table	—
Save results for Automation Batch	—
Change default quantitation method integration algorithm	Quantifizierung: Optionen der Standardmethode ändern
Change default quantitation method integration parameters	Quantifizierung: Optionen der Standardmethode ändern
Enable project modified peak warning	—
Add samples	Quantifizierung: Proben zur Ergebnistabelle hinzufügen bzw. aus dieser entfernen
Remove selected samples	Quantifizierung: Proben zur Ergebnistabelle hinzufügen bzw. aus dieser entfernen
Export, import or remove external calibration	—
Modify sample name	Quantifizierung: Probenname ändern
Modify sample type	Quantifizierung: Probentyp ändern

Tabelle C-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS	Analyst Software
Modify sample ID	Quantifizierung: Proben-ID ändern
Modify actual concentration	Quantifizierung: Analyt-Konzentration ändern
Modify dilution factor	Quantifizierung: Verdünnungsfaktor ändern
Modify comments fields	Quantifizierung: Probenkommentar ändern
Enable manual integration	Quantifizierung: Manuell integrieren
Set peak to not found	—
Include or exclude a peak from the results table	Standards aus Kalibrierung ausschließen
Regression options	Quantifizierung: Regressionsparameter ändern
Modify the results table integration parameters for a single chromatogram	Quantifizierung: „Einfache“ Parameter in der Peak-Bewertung ändern, „erweiterte“ Parameter in der Peak-Bewertung ändern
Modify quantitation method for results table component	Quantifizierung: Methode der Ergebnistabelle bearbeiten
Create metric plot new settings	Quantifizierung: Einstellungen für die metrische Kurve ändern oder erstellen
Add custom columns	Quantifizierung: Formelspalten erstellen oder ändern
Set peak review title format	—
Remove custom column	Quantifizierung: Formelspalten erstellen oder ändern
Results table display settings	Quantifizierung: Genauigkeit der Ergebnistabellenspalte ändern, Sichtbarkeit der Ergebnistabellenspalte ändern, Ergebnistabelleneinstellungen ändern
Lock results table	—
Unlock results table	—
Mark results file as reviewed and save	—
Modify report template	Berichtsvorlagen-Editor: Berichtsvorlage erstellen/ändern
Transfer results to LIMS	—
Modify barcode column	—
Change comparison sample assignment	—

Tabelle C-1: Zuordnung von Berechtigungen (Fortsetzung)

SCIEX OS	Analyst Software
Add the MSMS spectra to library	Durchsuchen: Spektrum zu Bibliotheks-Datensatz hinzufügen
Project default settings	Quantifizierung: Globale (standardmäßige) Einstellungen ändern
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	Quantifizierung: Analyt-Gruppen erstellen, Analyt-Gruppen ändern
Browse for files	—
Enable standard addition	—
Set Manual Integration Percentage Rule	Quantifizierung: Prozent-Regel bei manueller Integration aktivieren oder deaktivieren

Datendatei-Prüfsumme D

Wir empfehlen den Nutzern, Datendatei-Prüfsummen für wiff-Dateien zu verwenden. Die Prüfsummenfunktion ist eine zyklische Redundanzprüfung, mit der die Integrität der Datendatei überprüft wird.

Wenn die „Data File Checksum“-Funktion aktiviert ist und eine Datendatei (wiff) erstellt wird, generiert die Software einen Prüfsummenwert mithilfe eines Algorithmus, der auf dem öffentlichen MD5-Verschlüsselungsalgorithmus basiert und speichert den Wert in der Datei. Wenn die Prüfsumme verifiziert wird, berechnet die Software die Prüfsumme und vergleicht die berechnete Prüfsumme mit der in der Datei gespeicherten Prüfsumme.

Der Prüfsummenvergleich kann zu drei Ergebnissen führen:

- Wenn die Werte übereinstimmen, ist die Prüfsumme gültig.
- Wenn die Werte nicht übereinstimmen, ist die Prüfsumme ungültig. Eine ungültige Prüfsumme zeigt an, dass entweder die Datei außerhalb der Software verändert oder die Datei bei aktivierter Prüfsummenberechnung gespeichert wurde und sich die Prüfsumme von der ursprünglichen Prüfsumme unterscheidet.
- Wenn die Datei keinen gespeicherten Prüfsummenwert enthält, wird keine Prüfsumme gefunden. Eine Datei hat keinen gespeicherten Prüfsummenwert, weil die Datei mit deaktivierter „Data File Checksum“-Funktion gespeichert wurde.

Hinweis: Der Benutzer kann die Prüfsumme mithilfe der Analyst Software überprüfen. Siehe die Dokumentation für die Analyst-Software.

Aktivieren oder Deaktivieren der Funktion „Data File Checksum“

1. Öffnen Sie den Arbeitsbereich „Configuration“.
2. Klicken Sie auf **Projects**.
3. Erweitern Sie ggf. **Data File Security**.
4. Aktivieren Sie das Kontrollkästchen **Enable checksum writing for wiff data creation**, um die Funktion „Data File Checksum“ zu aktivieren. Um die Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen.

Kontaktangaben

Kundenschulung

- In Nordamerika: NA.CustomerTraining@sciex.com
- In Europa: Europe.CustomerTraining@sciex.com
- Die Kontaktinformationen für Länder außerhalb der EU und Nordamerikas finden Sie unter sciex.com/education.

Online-Lernzentrum

- SCIEX Now Learning Hub

SCIEX Support

SCIEX und seine Vertretungen beschäftigen weltweit einen Stab an ausgebildeten Servicekräften und technischen Spezialisten. Der Support kann Fragen zum System oder anderen auftretenden, technischen Problemen beantworten. Weitere Informationen finden Sie auf der SCIEX-Website unter sciex.com, oder kontaktieren Sie uns unter:

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

Cybersicherheit

Die aktuellsten Hinweise zur Cybersicherheit von SCIEX-Produkten finden Sie unter sciex.com/productsecurity.

Dokumentation

Diese Version des Dokuments ersetzt alle vorherigen Versionen.

Für die Anzeige des Dokuments wird der Adobe Acrobat Reader benötigt. Um sich die neueste Version herunterzuladen, besuchen Sie https://get.adobe.com/reader.

Softwareproduktdokumentationen entnehmen Sie den Versionshinweisen oder dem mit der Software mitgelieferten Software-Installationshandbuch.

Informationen zur Hardware-Produktdokumentation finden Sie auf der Dokumentations-DVD für das System oder die Komponente.

Die neuesten Versionen der Dokumentationen sind auf der Website von SCIEX unter sciex.com/customer-documents verfügbar.

Kontaktangaben

Hinweis: Wenn Sie eine kostenlose gedruckte Ausgabe dieses Dokuments wünschen, wenden Sie sich bitte an sciex.com/contact-us.